

## On the Limitation of Embedding Cryptographic Signature at Physical Layer for Primary Transmitter Authentication

**Saranya**

M.Tech Scholar

SITAMS

Chittoor – India

**Abstract:** Recently, an interesting primary transmitter authentication scheme was proposed. The main idea of this scheme is to have the primary transmitter embed cryptographic authentication tag at the physical layer. There are a number of features that make this scheme attractive. It reveals the effective coverage areas for the primary and secondary receivers before and after applying this scheme. During the process, it reveals a serious limitation of this scheme, which may prohibit its application in practice.

**Keywords:** Wireless security, authentication, cognitive radio Network.

### I. INTRODUCTION

A Serious security threat to a cognitive radio (CR) network is the so-called Primary User Emulation (PUE) attack. Under PUE attack, an adversary emulates the primary transmitter, and thus effectively shutting off potential opportunity for secondary users to access the spectrum. In the presence of PUE attack, spectrum sensing mechanisms based on either energy or feature detection is incapable of offering truthful results. Thus, an effective primary transmitter authentication method is needed.

Liu, proposed an authentication scheme that integrates cryptographic and wireless link signatures. At the heart of this scheme is a “helper node”, which is in close proximity to the primary transmitter. The helper node is assumed to share similar location-based channel impulse response (temporal link signature) to that of the primary transmitter. A secondary user first authenticates the helper node through its cryptographic signature. Then the secondary user is able to authenticate a primary user based on the temporal link signature that it receives from the helper node. A strong assumption of this scheme is that no attacker is allowed to being close proximity to the primary transmitter. Another concern of this scheme is potential single point of failure at the helper node.

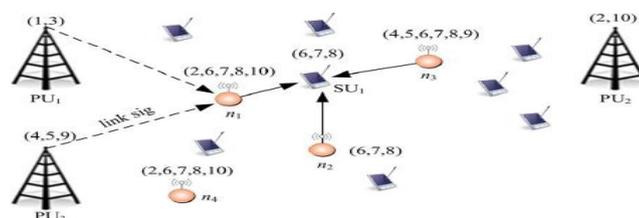


Fig. 1. System Architecture

Very recently, Tan et al. proposed an interesting authentication scheme that eliminates the need of a helper node. A neat idea in their scheme is to have the primary transmitter embed cryptographic authentication tag at the physical layer through either Modulation or channel coding (more details will be given in Section II). This information embedding process is equivalent to slightly perturbing the original signal purposely in a systematic manner. A secondary user will be able to extract

the embedded authentication tags and perform primary transmitter authentication, while a primary receiver is expected to decode the slightly perturbed signal by treating the embedded additional information as noise.

For the ease of exposition, we abbreviate the scheme ECS-PL (for Embedded Cryptographic Signature at the Physical Layer). At first glance, ECS-PL is appealing in a number of ways. First, ECS-PL is purely based on cryptographic signature, which is considered most effective in identifying PUE attack. Second, ECS-PL operates at the physical layer, and makes no requirement on upper layer compatibility between primary transmitters and secondary users for authentication. Such physical layer approach can support diverse population of secondary users under different upper layer protocols, as long as they understand physical layer signals. Third, it only requires a small modification of signal at the primary transmitter (i.e., TV tower). It does not require setting up any additional infrastructure such as the helper node. As a result, it eliminates any pitfalls associated with a helper node. Finally, it is transparent to primary receivers, in the sense that no hardware/software modification is needed at primary receivers. Existing primary receivers are still able to decode their received Signals as the embedded tag information is treated as noise.

A performance analysis of ECS-PL focusing on user data error rate (for primary receivers) and authentication tag error rate (for secondary receivers). Investigate ECS-PL from a different perspective. The effective coverage areas for the primary receivers and secondary users under ECS-PL. Specifically, we focus on physical layer modulation based on QPSK and investigate how to embed authentication tag bits without significant reduction in the coverage area for the primary receivers. That is, the upper bound for the phase shift required to embed authentication tag bits in QPSK modulation so as to maintain a similar size of effective coverage area for primary receivers. Based on this upper bound, the effective coverage area for the secondary receivers will be significantly reduced, rendering a large percentage of secondary users unable to perform authentication function, which violates the goal of ECS-PL scheme. Surprisingly, our finding is independent of some important system parameters such as primary transmitter power, bit rate, antenna heights and gains, and noise spectral density, among others.

## II. EMBEDDING CRYPTOGRAPHIC SIGNATURE INTO PHYSICAL LAYER MODULATION

The basic idea of ECS-PL is to embed the cryptographic authentication tag as noise into signal at the primary transmitter. Such embedded information may be considered as noise to a primary receiver. If such man-made noise is kept low enough, a primary receiver will be able to filter out such noise and recover the original transmitted signal. On the other hand, if such noise is above certain threshold, a secondary receiver (CR-based) will be able to extract the embedded cryptographic information from the received signal and use it to authenticate the primary transmitter. ECS-PL can be done either in modulation or channel coding and we focus on modulation in this letter. In the rest of this section, we briefly review ECS-PL with QPSK modulation.

QPSK modulation of signals, QPSK is a basic digital modulation technique that converts user data stream into transmitted signals (over a carrier frequency) with different phases. Specifically, user's digital data stream is broken into a sequence of two-bit pairs, with each pair being among the set of {11, 01, 00, 10} possible pairs. Then QPSK maps each two bit pair into one of the four phases on a QPSK constellation as shown in Fig. 2(a). Depending on which two-bit pair is used, a QPSK modulated carrier signal (over a symbol time interval  $T_s$ ) can be represented by

$$S_i(t) = \sqrt{\frac{2E_s}{T_s}} \cos(2\pi f_c t + (2i - 1)\frac{\pi}{4}) \quad i = 1, 2, 3, 4,$$

Where  $f_c$  is the carrier frequency and  $E_s$  is energy per symbol. At receiver side, the received signal (which is the sum of original signal plus noise) will fall into one of the four zones of QPSK constellation. Depending on which zone the received signal falls into, a corresponding two-bit pair will be determined. Obviously, if the noise level is not too high, the received signal will fall into its expected zone with high probability.

Embedding Authentication Tags into Modulated Signals, the basic idea of embedding cryptographic information in a modulated signal is to perturb the pre-defined QPSK phases toward the horizontal I-axis or the vertical Q-axis by an “additional” small phase  $\theta$  depending on the underlying tag bit (0 or 1). Specifically, in Fig. 2(b), for any of the four QPSK signals, if we want to embed a tag bit of 1 into the signal, we will shift an additional phase of  $\theta$  toward the vertical Q-axis. Likewise, if we want to embed a tag bit of 0 into the signal, we will shift an additional phase of  $\theta$  toward the horizontal I-axis. For decoding at the secondary receiver, we divide the  $2\pi$  phase into four Tag-Regions, which is a  $\pi/4$  counter clockwise phase shift of the four QPSK-Zones. Depending on which Tag-Region the received signal falls into, a secondary receiver will determine the corresponding tag bit. Note that after such phase perturbation, a transmitted signal will carry two pieces of information: the user data stream (a two-bit pair) and authentication tag information.

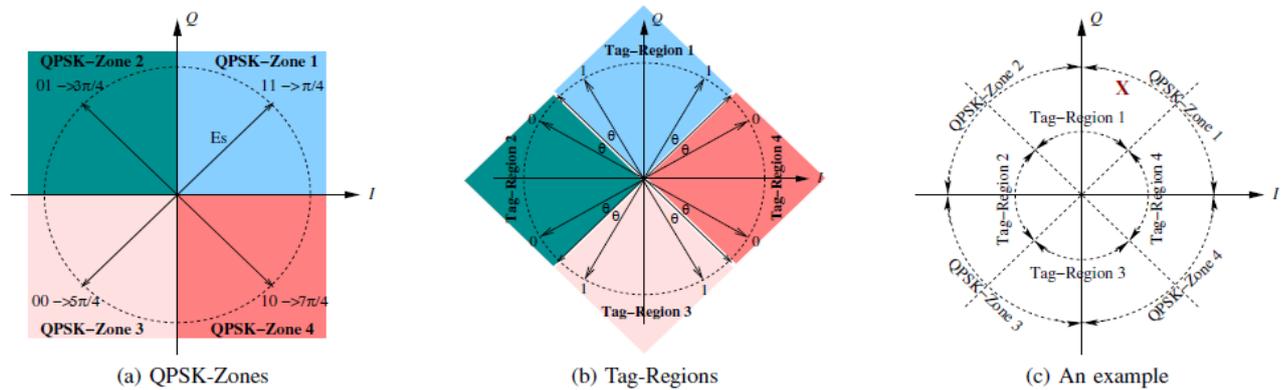


Fig. 2: A Schematic illustrating embedding cryptographic signature into QPSK modulation.

Recovering Signals and Authentication Tags at Primary and Secondary Receivers, for the modulated signal, additional noise will be added to the signal at a receiver. Depending on which QPSK-Zone the received signal falls into, a primary receiver will determine the corresponding user data (two-bit symbol). At the same time, depending on which Tag-Region the same received signal falls into, a secondary receiver will determine the corresponding tag information (one bit).

As an example, suppose a user data of 11 is being transmitted and a tag bit of 1 is to be embedded in the signal. Then the received signal is

$$\bar{S}(t, \theta) = \sqrt{\frac{2E_s}{T_s}} \cos\left(2\pi f_c t + \frac{\pi}{4} + \theta\right) + W(t),$$

Where,  $W(t)$  is white Gaussian noise with zero mean and power spectral density  $N0/2$ . Referring to Fig. 2(c), suppose the received signal falls at “X”. Since this point is in QPSK Zone 1, a primary receiver can determine the received user data being 11. At the same time, a secondary receiver can determine that the tag bit is 1 since the point is in Tag-Region 1. Clearly,  $\theta$  is a critical parameter. We will show how to set  $\theta$  in the next section.

### III. CALCULATING EFFECTIVE COVERAGE AREAS

A comprehensive analysis of data and tag error probabilities for primary and secondary receivers, in this section, we focus on the impact of ECS-PL on the effective coverage areas for primary and secondary a user, which was not explored but is vital to the successful application of this scheme in practice.

We assume the signal propagation between a primary transmitter (e.g., TV tower) and a receiver (either primary or secondary) follows a two-ray model (attenuation over reflecting surface) [5, Chapter 3], i.e.

$$p_r = \left[ \frac{h_t h_r}{d^2} \right]^2 \frac{(G_t G_r)}{L_0} p_t,$$

Where  $p_t$ ,  $h_t$  and  $G_t$  are the signal power, antenna height and gain of the primary transmitter,  $p_r$ ,  $h_r$  and  $G_r$  are the signal power, antenna height and gain of a receiver;  $d$  is the distance between the transmitter and receiver, and  $L_0$  is a parameter for other losses expressed as a relative attenuation factor.

---

### Procedure 1 Computing $A_p$

---

**Input:**  $p_t, h_t, G_t, h_r, G_r, P_s, L_0, N_0$  and  $B_r$

**Output:**  $R_p, A_p$

- 1: Compute  $E_b$  based on (2);
  - 2: Compute  $p_r$  based on (3);
  - 3: Compute  $d$  based on (1);
  - 4: **return**  $R_p = d, A_p = \pi(R_p)^2$ .
- 

---

### Procedure 2 Computing $A_p^{\text{ECS-PL}}$

---

**Input:**  $p_t, h_t, G_t, h_r, G_r, P_s, L_0, N_0, B_r$  and  $\theta$

**Output:**  $R_p^{\text{ECS-PL}}, A_p^{\text{ECS-PL}}$

- 1: Compute  $E_b$  based on (4);
  - 2: Compute  $p_r$  based on (3);
  - 3: Compute  $d$  based on (1);
  - 4: **return**  $R_p^{\text{ECS-PL}} = d, A_p^{\text{ECS-PL}} = \pi(R_p^{\text{ECS-PL}})^2$ .
- 

---

### Procedure 3 Computing $A_s^{\text{ECS-PL}}$

---

**Input:**  $p_t, h_t, G_t, h_r, G_r, P_s, L_0, N_0, B_r, \theta, P_e^{\text{tag}}, \text{BCH}(n^{\text{tag}}, k^{\text{tag}}, t^{\text{tag}})$  and  $L$

**Output:**  $R_s^{\text{ECS-PL}}, A_s^{\text{ECS-PL}}$

- 1: Compute  $P_{cw}^{\text{tag}}$  based on (7);
  - 2: Compute  $P_t$  based on (6);
  - 3: Compute  $E_b$  based on (5);
  - 4: Compute  $p_r$  based on (3);
  - 5: Compute  $d$  based on (1);
  - 6: **return**  $R_s^{\text{ECS-PL}} = d, A_s^{\text{ECS-PL}} = \pi(R_s^{\text{ECS-PL}})^2$ .
- 

## 1. Effective Coverage Area for Primary Receivers before ECS-PL

We first calculate the effective coverage area of the primary transmitter before ECS-PL scheme is employed. Denote this area as  $A_p$  and its radius (transmission range) as  $R_p$ . Denote  $P_s$  as the symbol error rate at a primary receiver. Then we have [5, Chapter 9]

$$P_s \simeq \text{erfc} \left( \sqrt{\frac{E_b}{N_0}} \right),$$

Where  $\text{erfc}$  is the complimentary error function,  $E_b/N_0$  is energy per bit to noise power spectral density ratio at a receiver. So once we have a target  $P_s$  for a given  $N_0$ , we can obtain energy per bit  $E_b$ . Once we have  $E_b$ , we can calculate the received signal power as

$$p_r = E_b B_r,$$

Where  $B_r$  is the bit rate, with  $p_r$  and (1), we can obtain  $d$ , which is also  $R_p$ . We summarize the above steps in Procedure 1.

## 2. Effective Coverage Area for Primary Receivers after ECS-PL

$$P_s \simeq \frac{1}{2} \text{erfc} \left( \sqrt{\frac{E_b}{N_0}} (\cos \theta - \sin \theta) \right) + \frac{1}{2} \text{erfc} \left( \sqrt{\frac{E_b}{N_0}} (\cos \theta + \sin \theta) \right)$$

After ECS-PL is employed, signal symbol error rate is given by [4]: compute the effective transmission range (denoted as

$R_p^{\text{ECS-PL}}$ ) as well as the coverage area (denoted as  $A_p^{\text{ECS-PL}}$ ) for primary receivers after ECS-PL is employed. We summarize the steps in Procedure 2.

### 3. Effective coverage area for secondary receivers after ECS-PL

After ECS-PL is employed, secondary receivers will receive the same signal as primary users but are only interested in decoding the tag information for authentication.

The tag bit error rate, denoted as  $P_t$ , is given by [4]:

$$P_t \simeq \frac{1}{2} \operatorname{erfc} \left( \sqrt{\frac{E_b}{N_0}} (\cos \theta) \right) + \frac{1}{2} \operatorname{erfc} \left( \sqrt{\frac{E_b}{N_0}} (\sin \theta) \right)$$

Even more important than  $P_t$  is the tag error rate, denoted as  $P_e^{\text{tag}}$ , which is defined as the probability of having one or more bits in error in the  $L$ -bit authentication tag and should be kept extremely low, e.g., below  $10^{-10}$ . Such stringent requirement is due to the fact that an authentication tag (with  $L$  bits) is a cryptographic hash value, which cannot tolerate even a single bit error.

To keep  $P_e^{\text{tag}}$  low, error correcting codes (ECC) can be used. First, a  $L$ -bit authentication tag is broken up into a number of  $k^{\text{tag}}$ -bit segments. Under ECC, each  $k^{\text{tag}}$ -bit segment is encoded into  $n^{\text{tag}}$ -bit codeword, which can correct up to  $t^{\text{tag}}$ -bit errors. Denote  $P_{cw}^{\text{tag}}$  as the probability that the received  $n^{\text{tag}}$ -bit codeword is in error. Then  $P_e^{\text{tag}}$  is upper bounded by [6, Chapter 3]:

$$P_{cw}^{\text{tag}} \leq \sum_{i=t^{\text{tag}}+1}^{n^{\text{tag}}} \binom{n^{\text{tag}}}{i} P_t^i (1 - P_t)^{n^{\text{tag}}-i},$$

Where  $P_t$  is the tag bit error rate in (5). With  $P_{cw}^{\text{tag}}$ ,  $P_e^{\text{tag}}$  can be further bounded by [4]:

$$P_e^{\text{tag}} \leq 1 - (1 - P_{cw}^{\text{tag}})^{\frac{L}{k^{\text{tag}}}}$$

So to achieve  $P_e^{\text{tag}}$  on the tag information, we can calculate the maximum  $P_{cw}^{\text{tag}}$  from (7). With this  $P_{cw}^{\text{tag}}$ , we can calculate  $P_t$  in (6). Then, we can follow the same token as in Procedure 1 to obtain the effective transmission range (denoted as  $RECS\text{-}PL_s$ ) and coverage area (denoted as  $AECS\text{-}PL_s$ ) for secondary receivers. We summarize the steps in Procedure 3.

Guideline for Setting  $\theta$  — Putting Everything Together

For a given  $\theta$  (see Fig. 1(b)), it is not hard to see that  $A_p^{\text{ECS-PL}}$  will be smaller than  $A_p$  under the same settings for other parameters.<sup>1</sup> This is intuitive as the perturbation on the QPSK constellation (to embed authentication tag) is considered additional noise by a primary receiver. But to comply with FCC requirements, the impact of ECS-PL on  $A_p^{\text{ECS-PL}}$  should be minimal, meaning that  $AECS\text{-}PL_p$  should be comparable to  $A_p$ , e.g.,  $A_p^{\text{ECS-PL}} \geq 0.95 \cdot A_p$  or even higher. Such requirement offers a guideline on how to set  $\theta$ . Once we have determined  $\theta$ , we investigate

$A_s^{\text{ECS-PL}}$  TABLE I: Results for  $(1 - \frac{A_s^{\text{ECS-PL}}}{A_p})$  and  $\theta$  under different BCH codes and  $P_s$  with  $A_p^{\text{ECS-PL}} = 0.95 \cdot A_p$ .

BCH code, $P_s$	$\theta$	$(1 - \frac{A_s^{ECS-PL}}{A_p})$
(127, 50, 13), $2 \times 10^{-3}$	$\frac{\pi}{32}$	87.07%
(127, 50, 13), $2 \times 10^{-4}$	$\frac{\pi}{37}$	86.53%
(127, 50, 13), $2 \times 10^{-5}$	$\frac{\pi}{41}$	86.06%
(511, 10, 127), $2 \times 10^{-3}$	$\frac{\pi}{32}$	72.31%
(511, 10, 127), $2 \times 10^{-4}$	$\frac{\pi}{37}$	71.17%
(511, 10, 127), $2 \times 10^{-5}$	$\frac{\pi}{41}$	70.15%
(1023, 11, 255), $2 \times 10^{-3}$	$\frac{\pi}{32}$	68.71%
(1023, 11, 255), $2 \times 10^{-4}$	$\frac{\pi}{37}$	67.42%
(1023, 11, 255), $2 \times 10^{-5}$	$\frac{\pi}{41}$	66.28%

#### IV. MAIN RESULT

In this section, we investigate AECS-PL  $s$  in relative to  $A_p$ . The guideline on how to set  $\theta$  was discussed in the last section. Specifically, based on Procedure 1, we can calculate  $A_p$ . Then by setting AECS-PL  $p = 0.95 \cdot A_p$ , we can use Procedure 2 in a reverse manner to calculate  $\theta$ . Based on this  $\theta$ , we can use Procedure 3 to calculate AECS-PL  $s$ . Since we are interested in finding how much smaller of AECS-PL  $s$  in relative to  $A_p$ , we calculate  $(1 - \text{AECS-PL } s / A_p)$ . Interestingly, this calculation is independent of the settings for parameters  $pt$ ,  $ht$ ,  $Gt$ ,  $hr$ ,  $Gr$ ,  $L0$ ,  $N0$  and  $Br$ , as they show up both on the numerator and denominator and cancel out. To generate authentication tag, we assume SHA-1 is used (with a length of 160 bits). The only remaining parameters that need to be set are data symbol error rate  $P_s$ , authentication tag error rate  $P_{tag e}$ , and BCH code for ECC.

- $P_s$ : We will consider three bit error rates that a primary Receiver can tolerate:  $10^{-3}$ ,  $10^{-4}$  and  $10^{-5}$ . These correspond to approximately  $2 \times 10^{-3}$ ,  $2 \times 10^{-4}$ , and  $2 \times 10^{-5}$  for symbol error rate  $P_s$ , respectively, due to QPSK.
- $P_{tag e}$  is set to  $10^{-10}$ , same as that in [4].
- BCH code: We tried all primitive BCH codes available in [6, Appendix C] and the results are consistent. For illustration, we show our results for three sets of BCH codes in the form of  $(ntag, ktag, itag)$  in Table I. The first set of code (127, 50, 13) was used in [4]. The codes (511, 10, 127) and (1023, 11, 255) are not commonly used but are extremely powerful. They are chosen to represent extreme BCH codes in our study. Table I shows our numerical results. We find that for all cases,  $\theta$  is quite small and  $(1 - \text{AECS-PL } s / A_p)$  is quite high, showing a significant reduction of effective area for secondary receivers. Assuming uniform secondary user density in the area, this means that *there is a very large percentage (over 65%) of secondary users unable to perform primary transmitter authentication*. Although more powerful BCH codes help reduce  $(1 - \text{AECS-PL } s / A_p)$  (from 86% to 67% for  $P_s = 2 \times 10^{-4}$ ), there is hardly much further improvement one can expect as we have exhausted all public available BCH codes. It is worth pointing out that if FCC requires more stringent area coverage for AECS-PL  $p$ , e.g.,  $\text{AECS-PL } p = 0.99 \cdot A_p$ , then  $(1 - \text{AECS-PL } s / A_p)$  will become even worse (an increase). For example, under BCH code (127, 50, 13) and  $P_s = 2 \times 10^{-3}$ ,  $(1 - \text{AECS-PL } s / A_p)$  increases to 95% when  $\text{AECS-PL } p = 0.99 \cdot A_p$ , meaning that 95% of secondary receivers are not able to authenticate the primary transmitter. The large reduction of AECS-PL  $s$  in our findings can be explained by the very small value of  $\theta$  one can choose in order to ensure AECS-PL  $p$  is comparable to  $A_p$ . This will result in large tag bit error rate  $P_t$  as well as tag error rate  $P_{tag e}$  (even with ECC). On the other hand, there is a very high requirement on  $P_{tag e}$  (e.g.,  $10^{-10}$ ) as a single bit error in an authentication tag will render its useless. Under such environment, only a small percentage of secondary users that are very close to the primary transmitter will have adequate received signal power and decode the authentication tag correctly.

**V. CONCLUSION**

In this paper, we investigated a recently proposed primary transmitter authentication scheme that embeds cryptographic authentication information at the physical layer. We focused on the effective coverage areas for primary and secondary receivers under this scheme. We found that by requiring a similar size of coverage area for primary receivers before and after the scheme, the effective coverage area for secondary users must be much smaller than that for primary users. Consequently, a large percentage of secondary users are not able to decode the cryptographic signature for authentication. Interestingly, our finding is independent of some important system parameters such as primary transmitter power, signal bit rate, antenna heights and gains, and noise spectral density. Our findings show a fundamental limitation of the proposed physical layer authentication scheme and thus encourage further research in this important area.

**References**

1. R. Chen, J. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 1, pp. 25–37, Jan. 2008.
2. Y. Liu, P. Ning, and H. Dai, "Authenticating primary users' signals in cognitive radio networks via integrated cryptographic radio networks via integrated cryptographic and wireless link signatures," in *Proc. 2010 IEEE Symp. on Security and Privacy*, pp. 286–301.
3. B. Danev, H. Luecken, S. Capkun, and K. E. Defrawy, "Attacks on physical-layer identification," in *Proc. 2010 ACM WiSec*, pp. 89–98.
4. X. Tan, K. Borle, W. Du, and B. Chen, "Cryptographic link signatures for spectrum usage authentication in cognitive radio," in *Proc. 2011 ACM WiSec*, pp. 79–90.
5. V. K. Garg, *Wireless Communications and Networking*. Elsevier/Morgan Kaufmann Publishers, 2007.
6. S. Lin and D. J. Costello, *Error Control Coding*, 2nd edition. Pearson Prentice Hall, 2004.

**AUTHOR(S) PROFILE**

**B SARANYA**, received the B.E degree in Electronics & Communication Engineering from Priyadarshini Engineering College , Anna University , Chennai, Tamilnadu India and doing M.tech communication system final year in the Sreenivasa Institute of Technology & Management Studies Chittoor, JNTU University Anandhapur Andhra Pradesh, India in 2010 & 2013.