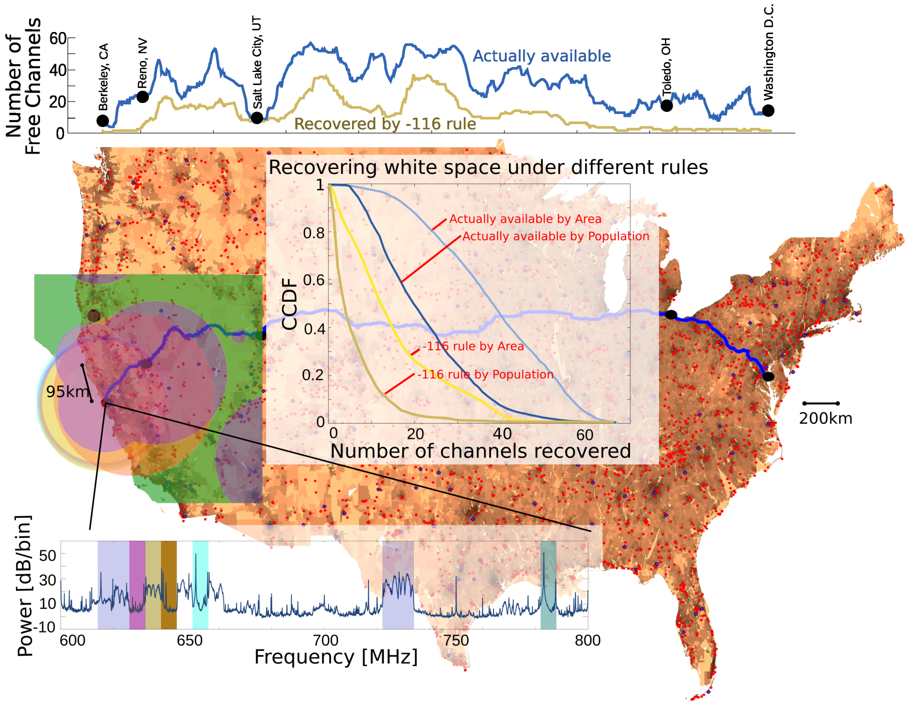
Kristen Ann Woyach, Anant Sahai, George Atia, and Venkatesh Saligrama,
"Crime and Punishment for Cognitive Radios,"
Fourty-sixth Allerton Conference on Communication, Control, and Computing, Sep. 2008.

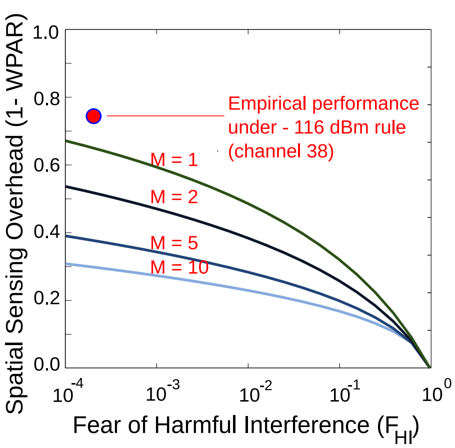
Paper available: www.eecs.berkeley.edu/∼sahai/Papers/CrimePunishmentAllerton08.pdf
Slides available: . . . /∼sahai/Presentations/CrimePunishmentAllerton08.pdf
This Handout: . . . /∼sahai/Presentations/CrimePunishmentAllerton08.H.pdf

Further discussion, related work, and references can be found in the paper.

1 Motivation



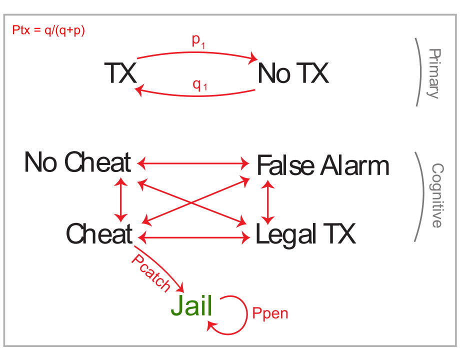
Starting from the San Francisco Bay Area on this map of the U.S. shaded by population density, we see that TV towers have footprints on the surrounding area that do not entirely overlap. The uncovered spaces are "holes" in spectrum usage that can be reclaimed by cognitive radios. As we take a virtual trip along Interstate 80, we see from the plot at the top that there are lots of channels not being used throughout the U.S. However, the central figure shows that there are somewhat fewer opportunities where most people live. This figure was created by Mubaraq Mishra.



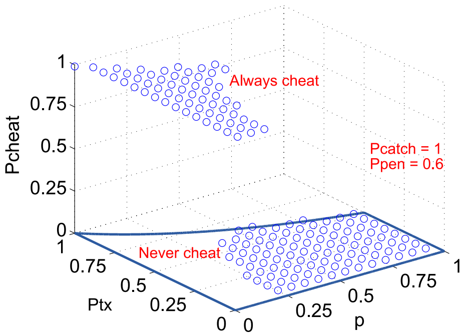
But how do we certify devices that take advantage of these "spectrum holes?" Although lab testing would be effective for a single radio sensing by itself, this plot shows that cooperative schemes are far more effective at recovering spectrum in most areas. Unfortunately, cooperative schemes are far harder to certify, perhaps requiring digging through thousands of lines of code to make sure an adversarial vendor is not trying to fool the test. In this paper, we propose an easily certified jail-based punishment mechanism that enables runtime policing. This figure was created by Mubaraq Mishra and Rahul Tandra. Both this and the previous figure appear in: A. Sahai, S.M. Mishra, R. Tandra, and K. Woyach, "Cognitive Radios for Spectrum Sharing," to appear in the *DSP Applications* column in the *IEEE Signal Processing Magazine* for January 2009.

2 Crime and Punishment

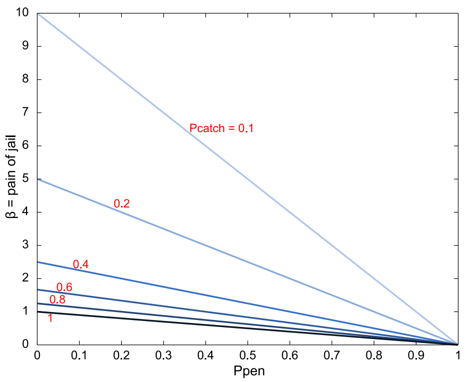
2.1 Single Band Model



A simple Markov chain is used to model primary and cognitive user behavior, employing a "spectrum jail" system to punish cognitive user misbehavior. The concept is to model the incentives involved in cheating, and to evaluate what an enforcement mechanism has to do in order to deter cognitive users from cheating. The top chain defines p and q which *characterize primary usage*. Cognitive users move in response to the primary users, choosing P_{cheat}, *the probability of cheating*, to maximize their utility — *the average time spent transmitting*. If in the cheating state, P_{catch} is *the probability of being caught and sent to jail*. Once in jail, P_{pen} *determines how long* ($\frac{1}{1-P_{pen}}$ *on average) the cognitive user must wait before rejoining the game*. The regulator can adjust P_{pen} and P_{catch} to deter cheating.



Typical cognitive user cheating behavior, when the primary is allowed to choose only P_{catch} and P_{pen}. The cheating behavior falls into one of two regimes: always cheating or never cheating, depending on the enforcement parameters. Note that if punishment is simply a time-out, there is no way to deter cheating when the primary is nearly always active (high $P_{TX} = q/(q+p)$) because the cognitive user will be not transmitting whether being honest or sitting in jail.

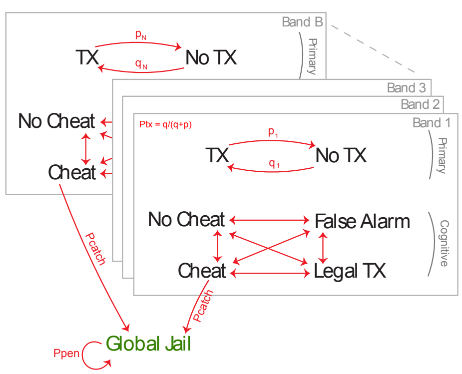


The regulator needs to set the enforcement parameter P_{pen} at certification time, and so it must work for any values of p and q, particularly the worst case when P_{TX} is very high. As noted above, time-outs alone are insufficient to deter cheating in this case. Therefore, we introduce β as *the additional pain of jail* set by the regulator to deter cheating regardless of primary transition characteristic. This figure shows just how high β must be (above the line, cheating is not in the cognitive users best interest)

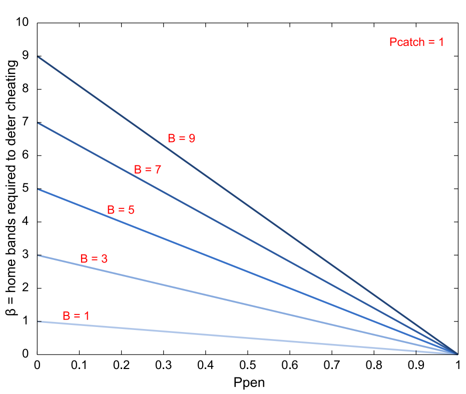
2.2 Multi-Band Model

Band:	Home	Expansion Band 1	Exp. Band 2	...	Exp. Band B	Total
Utility:	β	1	1	...	1	$\beta + B$

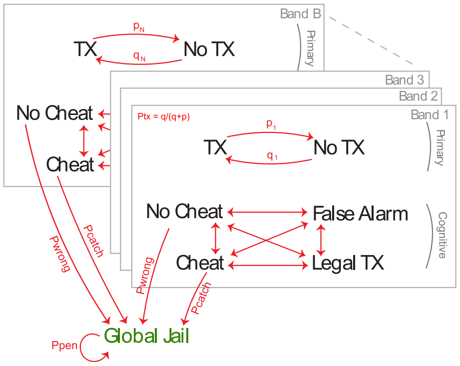
Alternatively, we can think of β as *the utility of a dedicated clean home band* the cognitive user has to stake as a guarantee against cheating. Cognitive use allows potential bandwidth expansion, *the maximum ratio of bands that a user is allowed to use in addition relative to its own dedicated home band*.



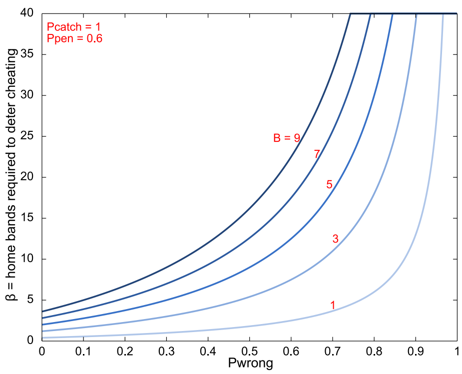
Consider a multi-band model, where there are B *bands a cognitive user may expand into*, and a Global Jail. If the cognitive user is caught cheating in any of the bands, it will go to a Global Jail where *the cognitive user is barred from using not only all of the expansion bands, but its home band as well.*

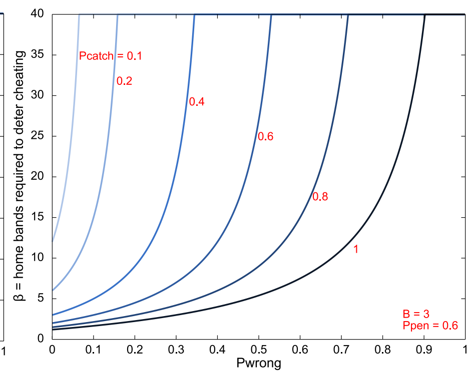


With multiple bands, the new β required to deter cheating even when all of the primaries are transmitting is shown here. Notice that this is simply B times the values before — when there are B bands to gain by cheating, there is B times the temptation. In this idealized model, setting P_{pen} high enough would allow the cognitive user to expand into a great many bands even if β were small.

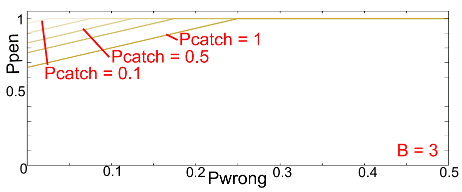


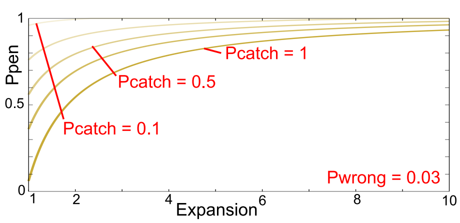
The model is now augmented to allow realistic uncertainty in the regulator's ability to catch and punish the correct cheater. P_{wrong} models *the probability of being wrongfully punished* (occurs when the wrong cognitive user is accused, the regulator employs collective punishment, or the cognitive user does not detect the primary transmission).



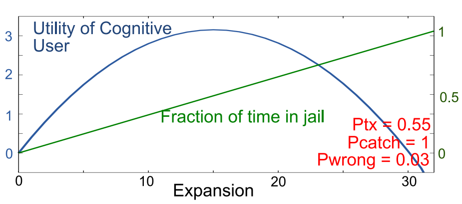


When the regulator can make mistakes, the β required to deter cheating when the primaries are all active all the time rises dramatically. Notice especially that when P_{wrong} gets close to P_{catch}, β goes to infinity. No amount of extra punishment is sufficient to deter cheating when you will be wrongfully sent to jail at the same rate anyway.

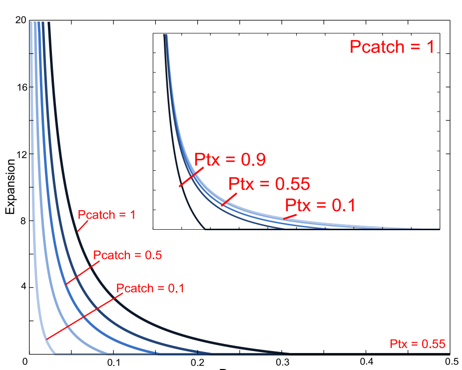




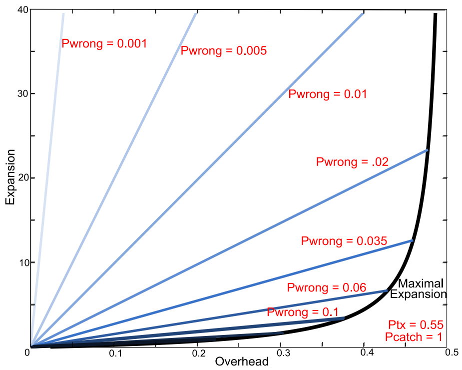
Because the β is the number of home bands a cognitive user has, it is presumably a quantity that cannot be changed. Therefore, the above condition on β can alternatively be thought of as a minimum P_{pen} for a given β necessary to deter cheating. Notice that as either P_{wrong} or the possible expansion B grows, the necessary P_{pen} approaches 1. It equals 1 when that expansion cannot be safely allowed.

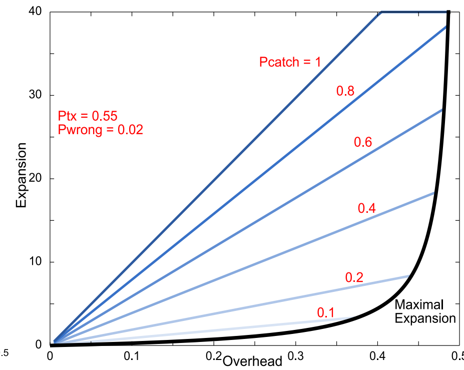


B and the resulting P_{pen}, for a particular P_{TX}, interact to determine how much utility the cognitive user will get. If choosing whether to expand at all, the cognitive user cares about the zero-crossing of this utility function. If it can choose its amount of expansion, it will try to maximize the utility function shown here. Notice that the maximum utility occurs around the point where the cognitive user is spending half of its time in jail.



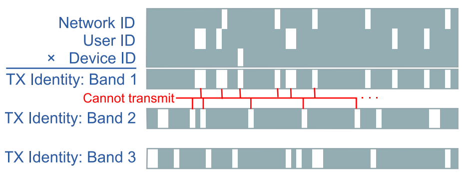
If the cognitive user can choose its expansion to maximize its utility, it will choose the values of B shown in this plot, varying P_{catch} in the larger figure and P_{TX} in the cutout. Notice that for large expansions, P_{wrong} must be very small, so it is of interest to the cognitive user to have a very good detector and demonstrate as such at certification time when its P_{pen} is set.



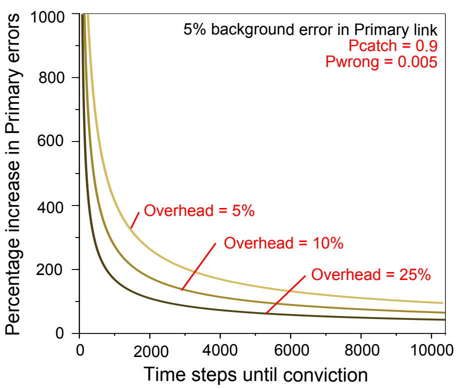


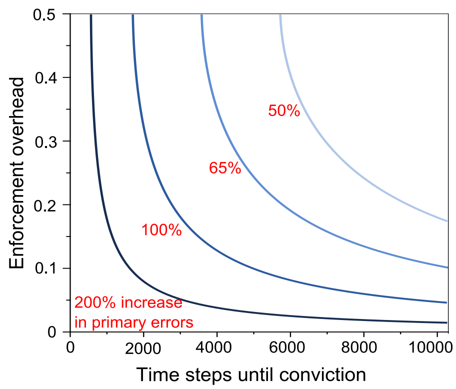
P_{wrong} dictates that the cognitive user will spend some time in jail despite honest use. We define the overhead as *the average amount of available bandwidth (spectrum the primaries are not currently using) the cognitive user cannot recover due to time spent in jail.* Notice that the overhead is never larger than 0.5 and for small overheads with large expansions, P_{wrong} must be extremely small.

3 Identity (Preview of DySpAN 2008)

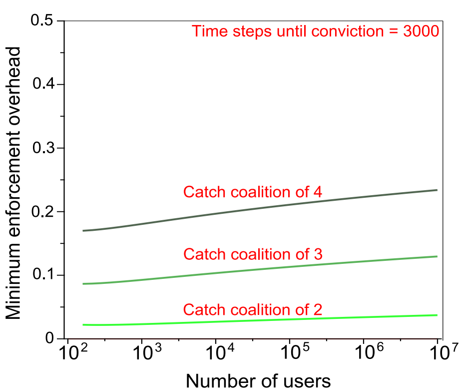


The small P_{wrong} required for large expansion above suggests that honest cognitive users will *want* to be catchable. Therefore, the will want to have identity. Here is an example of our proposed method to give radios identity: for each level of identity (user, device, network), the radio has a transmission pattern of slots when it is allowed and not allowed to transmit. The overall transmit identity is an AND rule on the individual identities — if any of the patterns say a slot cannot be used, the overall identity will not use that slot.





With the taboo-based identity described above, these plots show the overhead *(percentage of slots the radio cannot use because of the taboo-code)* and the percent increase in primary errors *(the degradation in the quality of service imposed on the primary user due to cheating by the cognitive user)* required for a particular number of steps until a single cheating cognitive user is convicted.



In reality, it is not enough to be able to convict a single known suspect. Many potential users could be out there and this figure shows an information-theoretic bound on the amount of overhead required to be able to narrow it down the appropriate parties within a short amount of time. The required overhead changes based on the size of the coalition *(number of users cheating at the same time)* that must be caught.

This talk is intended to bring out the following ideas:

- Although fully allocated, there exist many "holes" in spectrum that opportunistic use can help fill. But, enforcement with only *a priori* device-level certification seems difficult.
- It may be simpler to use a light-handed, incentive-based reactive enforcement scheme based on:
  - Radios obeying a "go directly to jail command" in which they are blocked from any wireless transmissions for a certain sentence that depends on the current capability of the radio for bandwidth expansion as well as the value of the home band they are able to stake.
  - Radios having their transmissions obey a "temporal profile" in which each radio has an individualized sequence of band-specific time-slots that are taboo to it.
- These requirements seem to be easy to certify and suffice to guarantee that no rational radio will intentionally cheat.