PHYSICAL LAYER SECURITY IN WIRELESS NETWORKS WITH ACTIVE EAVESDROPPERS

Arsenia Chorti[1,2]

[1]Department of Electrical Engineering, Princeton University

[2]Institute of Computer Science, Foundation for Research and Technology-Hellas

email: achorti@princeton.edu

1. INTRODUCTION

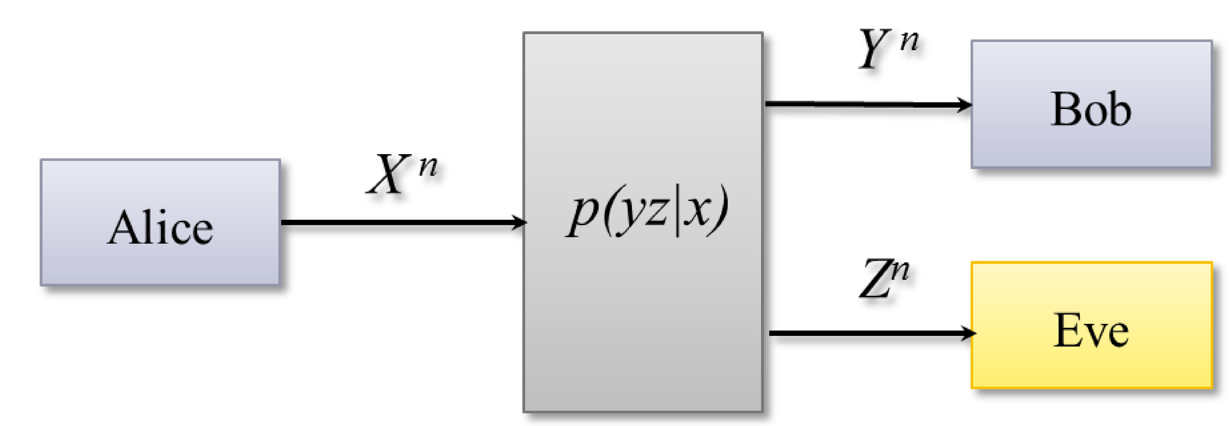
Perfect secrecy is achievable if there exists an SNR advantage at the legitimate user with respect to an eavesdropper.

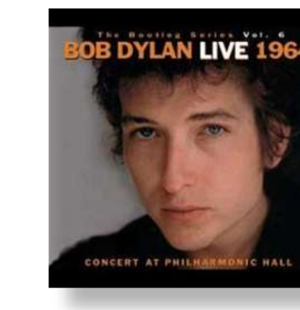
$$\boxed{C_S = \max_{\substack{p(u,x)\\ U-X-YZ}} \left(I(U;Y) - I(U;Z)\right)}$$

2. QUESTION

Can we incorporate perfect secrecy (quantitatively expressed through the secrecy capacity) in the Quality of Service (QoS) metrics of the network?

➡ Establish minimum secrecy capacity requirements for a given application.





3. NETWORK WITH ACTIVE EAVESDROPPERS

System Model:

- Centralized network with one management unit (base station)
- K registered users, amongst which E active eavesdroppers
- Users report channel gains

$$g_k = |h_k|^2 \text{ with pdf } f(g_k) = e^{-g_k}, \text{ and cdf } F(g_k) = 1 - e^{-g_k}, k = 1, \ldots, K$$

- BS transmits codewords x_k from a Gaussian codebook, with power p to the user with the highest SNR γ_k, where $\gamma_k = g_k p$
- Useful indices: *Best user, second best user, best eavesdropper*

$$a = \arg\max_{k \in \mathcal{K}} \gamma_k \qquad b = \arg\max_{k \in \mathcal{K}\setminus\{a\}} \gamma_k \qquad e = \arg\max_{k \in \mathcal{E}} \gamma_k$$

- **Secrecy capacity**: $C_s = \left(\log \frac{1+\gamma_a}{1+\gamma_e}\right)^+$

4. ACTIVE EAVESDROPPERS

Active eavesdropper: Appears as a registered user who reports forged Channel State Information (CSI) to the BS

Heuristic eavesdropper strategy

1. If it has the **highest SNR**, **i.e.** $e=a$
   - **Reports a lower SNR**
   - If the BS transmits to the second best user with index b, the eavesdropper can decode the secret message x_b
2. If it does **not** have the **highest SNR**
   - **It might report a higher SNR**
   - If the BS transmits to the eavesdropper, network resources are wasted

THE EAVESDROPPER CAN ALWAYS WIN!

5. GAME THEORETIC ANALYSIS

[CHORTI, PERLAZA, HAN, POOR, GLOBECOM'12]

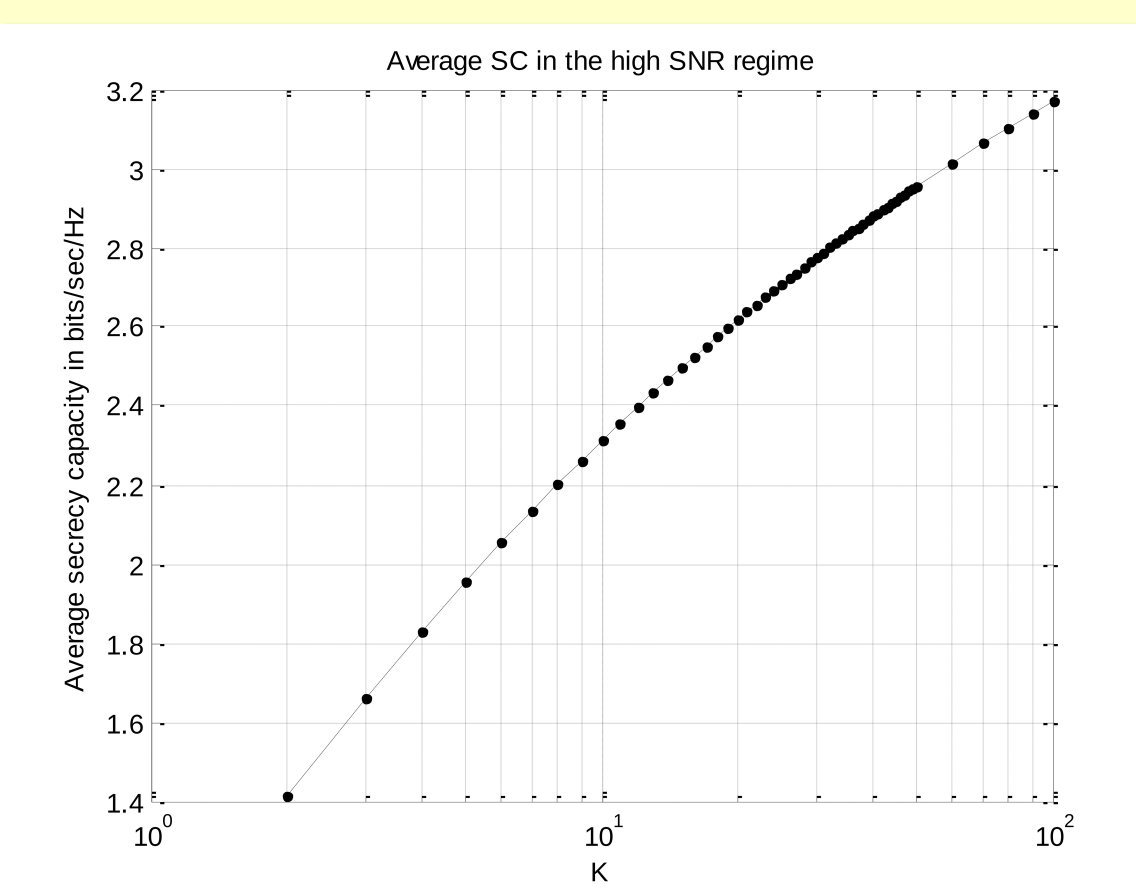
- The BS can potentially transmit *only* to the user with the highest *reported* SNR
- The active eavesdropper *always reports* a forged SNR value $\tilde{\gamma}_e = \gamma_e + \varepsilon$
- The BS and the eavesdropper have a common *utility function*

$$\boxed{u(p,\varepsilon) = \log \frac{1+g_a p}{1+g_e p} \mathbf{1}_{\{\gamma_a > \gamma_e + \varepsilon\}} = \log \frac{1+\gamma_a}{1+\gamma_e} \mathbf{1}_{\{\gamma_a > \tilde{\gamma}_e\}}}$$

u(p, ε)>0	***u(p, ε)=0***	***u(p, ε)<0***
❑The BS transmits to a legitimate user ❑Non zero secrecy capacity	❑The BS transmits to the eavesdropper ❑Network resources are wasted	❑The BS transmits to a legitimate user ❑Potential information leakage to the eavesdropper

- Average Secrecy Capacity $\langle C_s(\hat{\varepsilon}) \rangle = \int_0^\infty \int_{g_a + \frac{\hat{\varepsilon}}{p_{\max}}}^\infty \log \frac{1+g_a p_{\max}}{1+g_e p_{\max}} dF(g_e) dF_a(g_a)$

6. HIGH SNR REGIME



7. SECRECY CAPACITY BOUNDS

We assume that the reported channel gain $\tilde{g}_e$ deviates from the true value g_e by a quantity θ with pdf $p_\Theta(\theta)$

- The BS cannot distinguish between the legitimate user and the active eavesdropper
- Bounds on the secrecy capacity

$$\langle C_s \rangle_{\min(or\max)} = \min(or\max)\left\{\max_{P_1(\theta)} \int_{\tilde{g}_1-\theta-g_2}^{\infty} \log \frac{1+P_1(\tilde{g}_1-\theta)}{1+P_1 g_2} p_\Theta(\theta) d\theta,\right.$$

$$\left.\max_{P_2(\theta)} \int_{g_1-\tilde{g}_2-\theta}^{\infty} \log \frac{1+P_2 g_1}{1+P_2(\tilde{g}_2-\theta)} p_\Theta(\theta) d\theta,\right\}$$

- If the minimum secrecy capacity exceeds a threshold value, the BS transmits, otherwise no transmission takes place

8. CONCLUSIONS

The effect of an active eavesdropper was systematically evaluated through the use of game theoretic tools under a full CSI assumption. Our analysis suggests that in order to minimize the loss incurred by such attacks, side information is required. Interestingly, we found that in the high SNR regime, the network is insensitive to the passiveness or activeness of the attack. Finally, assuming a stochastic modeling of the behavior of the active eavesdropper is available, we have derived bounds for the instantaneous secrecy capacity that can be used to determine power allocation strategies.

ACKNOWLEDGEMENTS

This work was funded in part by the IOF "APLOE" (PIOF-GA-2010-274723) grant within the 7th Framework Program of the European Community and in part by the U. S. National Science Foundation Grant CNS-09-05398.