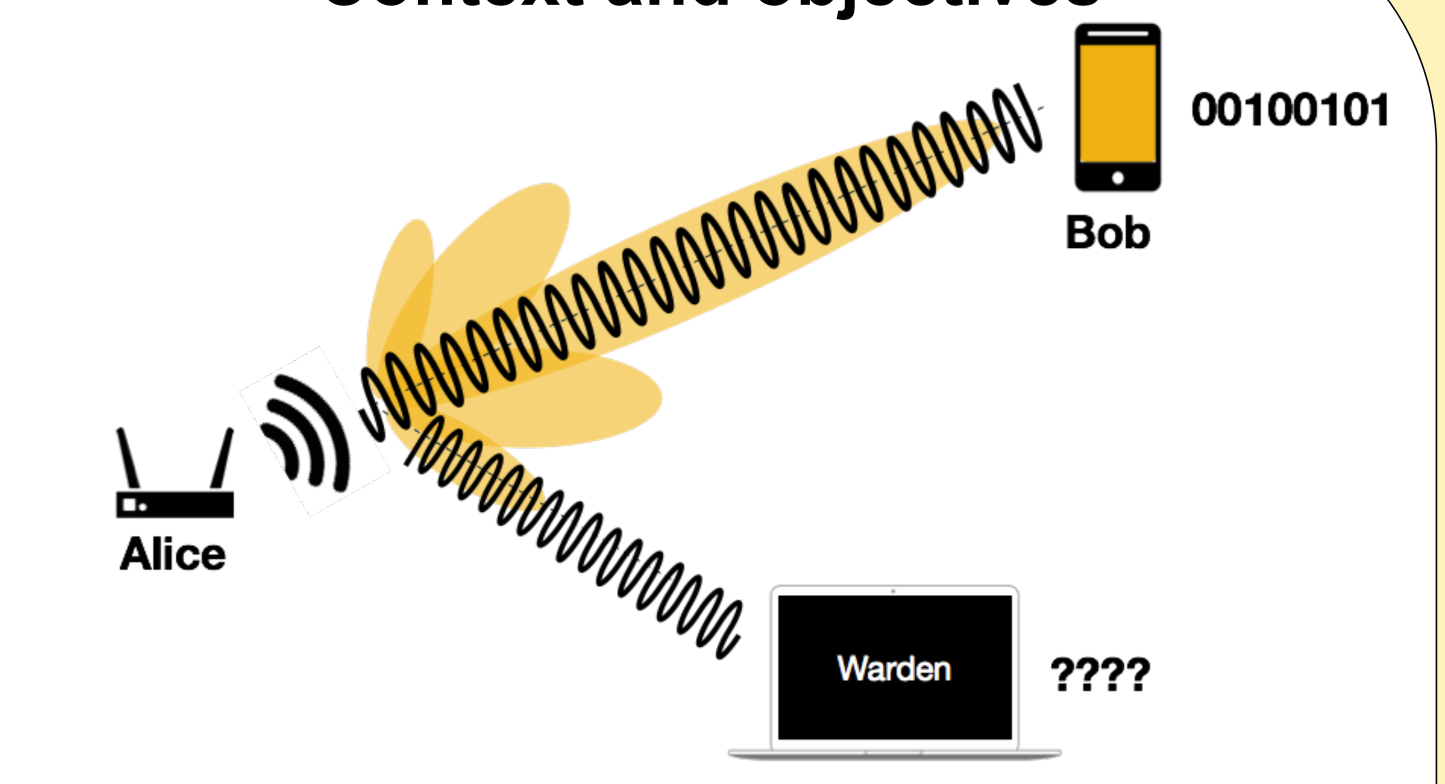
Towards stealth networks

PI: Matthieu Bloch, Georgia Institute of Technology
http://arcom.gatech.edu/research/stealth-networks

Context and objectives

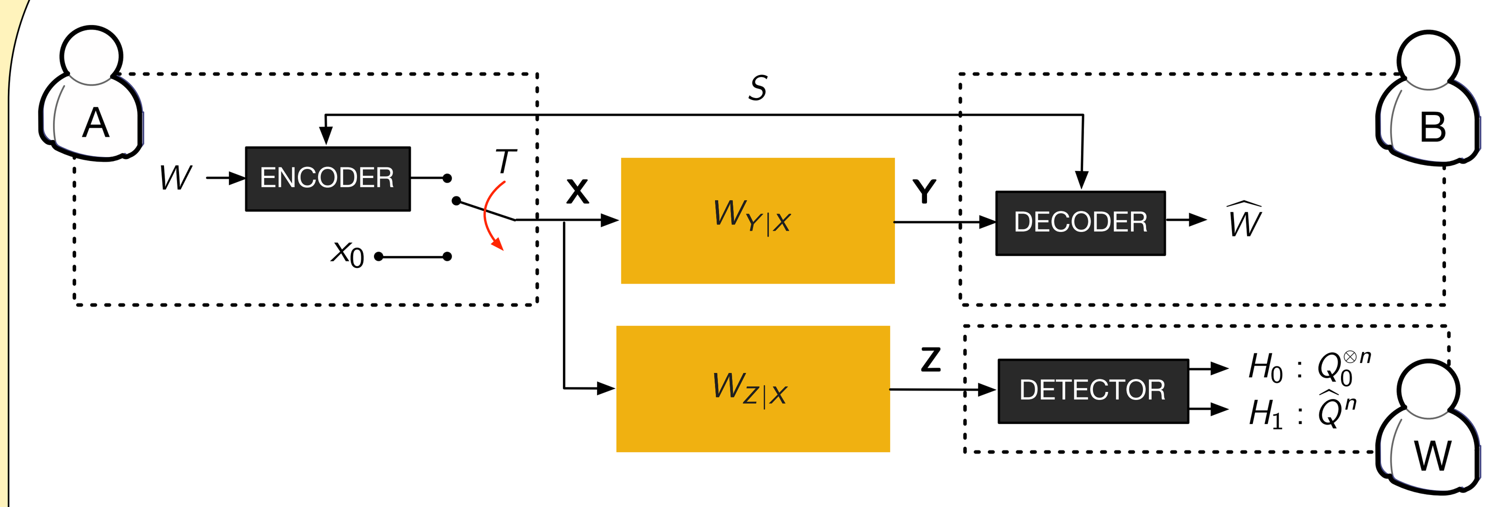


Many situations in which the *mere fact* of communicating should be *covert*

- Escaping monitoring from authoritarian entities
- Avoiding interference to primary users for spectrum sharing

How many bits can be transmitted reliably and covertly? What coding and signaling schemes should be used?

Information-theoretic modeling



Communicating parties connected by noisy channels. “No communication” represented by transmission of symbol x_0.

Communication could happen using publicly known codebook, possibly assisted by secret key *S*. Adversary is allowed to implement optimal Neyman-Pearson detector to detect communications.

Two fold objective

- Communicate reliably
- Ensure that optimal detector is no better than random guess

Approach

Information-theoretic covertness

- Use relative entropy to capture performance of best detector

Exploit *low-weight* codewords

- Communication can only escape detection if fraction of non-x_0 symbols is *sublinear*

Use error control codes to shape statistics

- The occurrence of non-x0 symbols should not exhibit predictable patterns
- Error control code can be *jointly* used to provide reliability and *resolvability*, i.e., induce i.i.d. statistics

Characterization of information theoretic limits of covert communication

Suitable normalization leads to notion of *covert capacity*. Reliable and covert communication possible if and only if number of message bits *log M* satisfies

$$\lim_{n\to\infty} \frac{\log M}{\sqrt{n\mathbb{D}\left(\widehat{Q}^n \| Q_0^{\otimes n}\right)}} = (1-\xi)\sqrt{\frac{2}{\chi_2(Q_1\| Q_0)}}\mathbb{D}(P_1\|P_0)$$

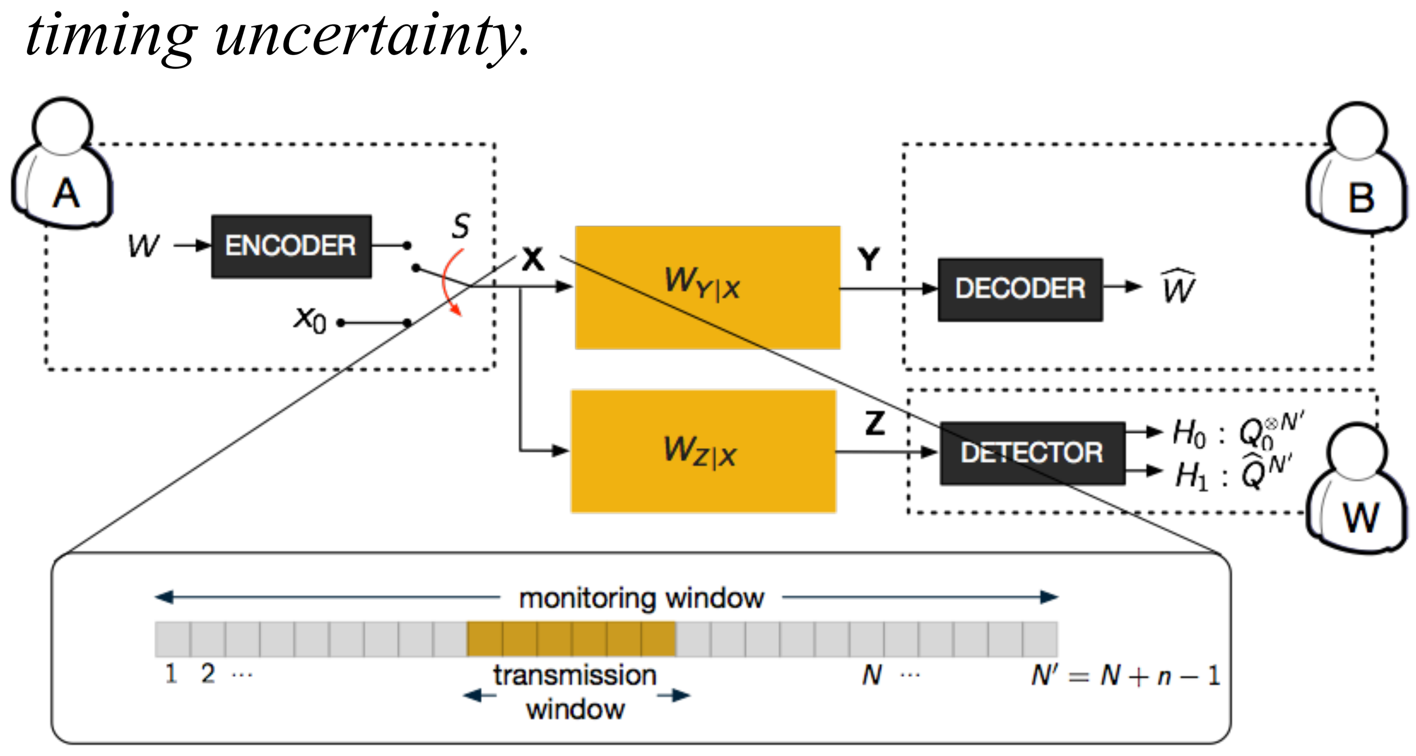
This also requires a number of key bits *log K*

$$\lim_{n\to\infty} \frac{\log K}{\sqrt{n\mathbb{D}\left(\widehat{Q}^n \| Q_0^{\otimes n}\right)}} = \sqrt{\frac{2}{\chi_2(Q_1\| Q_0)}}\left[(1+\xi)\mathbb{D}(Q_1\|Q_0) - (1-\xi)\mathbb{D}(P_1\|P_0)\right]^+$$

Vanishing rate of communication characterized by *square root law.* Similar to square root law in steganography, with role of cover played by channel noise

Effect of Timing Uncertainty

Square root law can be beaten by introducing *timing uncertainty.*



Hiding a transmission window of size *n* into monitoring window of size *N* improves throughput

$$N = \omega\left(\frac{n^2}{\log n}\right) \qquad \log M = O(\sqrt{n\log n})$$

Interested in meeting the PIs? Attach post-it note below!

National Science Foundation
WHERE DISCOVERIES BEGIN

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia

Georgia Institute of Technology