

Quantum-secure Covert Communication on Bosonic Channels

Nature Communications 6, 8620 (2015)

Raytheon BBN Technologies

Boulat A. Bash (boulat.bash@raytheon.com)
with Andrei H. Gheorghe (Harvard), Monika Patel
(Carl Zeiss), Jonathan L. Habif, Dennis Goeckel
(UMass), Don Towsley (UMass), and Saikat Guha

November 2, 2016

"This document does not contain technology or technical data
controlled under either the U.S. International Traffic in Arms
Regulations or the U.S. Export Administration Regulations."

Introduction

- Much of modern security research is dedicated to preventing unauthorized message decoding
 - Cryptography: exploit adversary's computational limitations
 - Information-theoretic secrecy: exploit adversary's physical limitations

Introduction

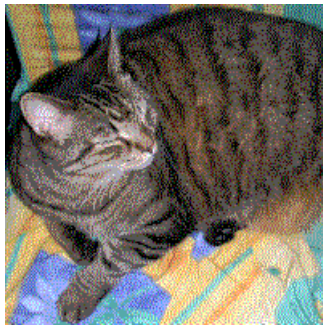
- Much of modern security research is dedicated to preventing unauthorized message decoding
 - Cryptography: exploit adversary's computational limitations
 - Information-theoretic secrecy: exploit adversary's physical limitations
- But what if that is not enough?
 - Social unrest: government may shut down any, especially encrypted, transmissions
 - Military: hide presence of any activity
 - Privacy intrusion: it's often the "meta-data" that is important
- **Covert communication** conceals **presence** of messages in the first place

Introduction

- Much of modern security research is dedicated to preventing unauthorized message decoding
 - Cryptography: exploit adversary's computational limitations
 - Information-theoretic secrecy: exploit adversary's physical limitations
- But what if that is not enough?
 - Social unrest: government may shut down any, especially encrypted, transmissions
 - Military: hide presence of any activity
 - Privacy intrusion: it's often the "meta-data" that is important
- **Covert communication** conceals **presence** of messages in the first place
- **What are the fundamental limits of covert communication?**
 - Need **quantum information theory** to study physical limits

Prior art: Steganography

- Why not use digital steganography?



message

⇒
embed



covertext

→
obtain

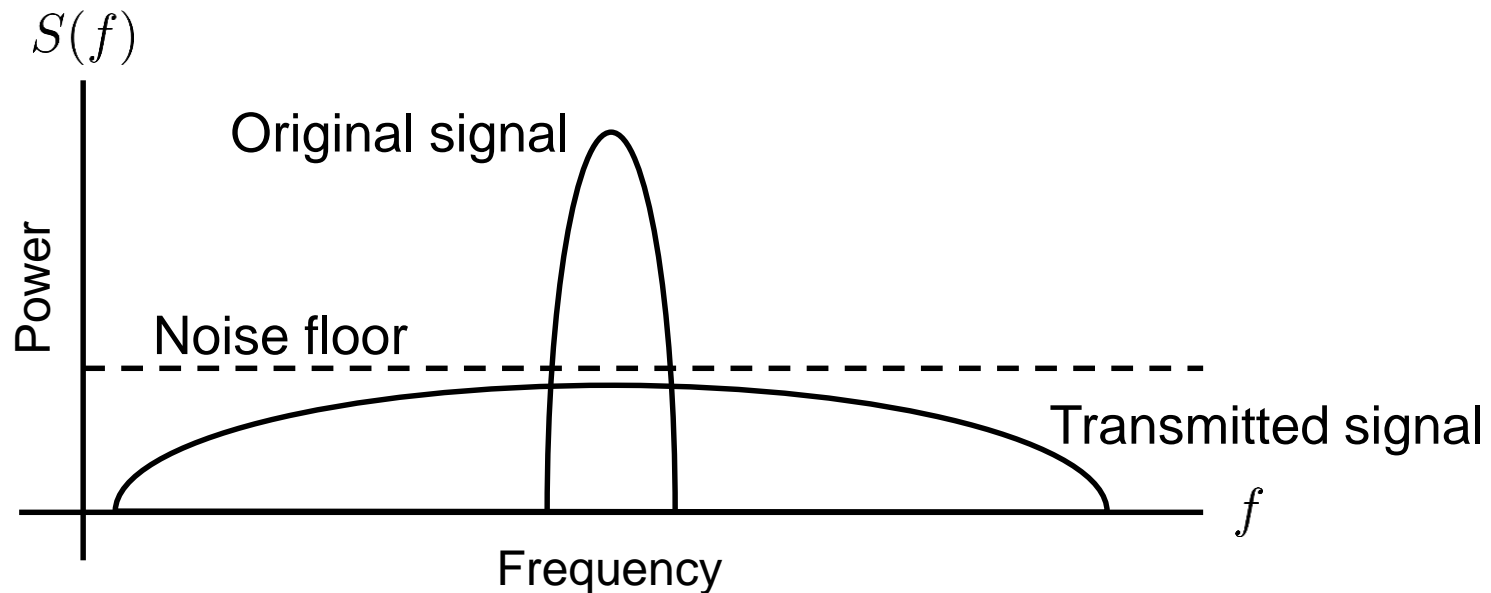


stegotext

Source: User Cyp, Wikipedia

- Embedding overwrites covertext noise, which we can't necessarily access in noisy communication channel scenario
- *Requires transmission of stegotext, inapplicable when transmissions are prohibited*

Spread spectrum communication



- **What is “safe” power level and how much can be transmitted without detection?**
 - Square root law for AWGN channels [Bash12, Bash13a]: must use average per-symbol power $P_f = O\left(1/\sqrt{n}\right)$ over n channel uses; transmit no more than $O(\sqrt{n})$ bits total
- Optical detection systems are quantum-noise limited: must use quantum mechanics to derive limits under the most powerful adversary permissible by physics

Outline

- Introduction
- Preliminaries
- Analysis of covert optical communication
- Experimental results
- Conclusion: Vision for Shadow Network Architecture

Covert Communication Model

- Alice has a noisy channel to Bob



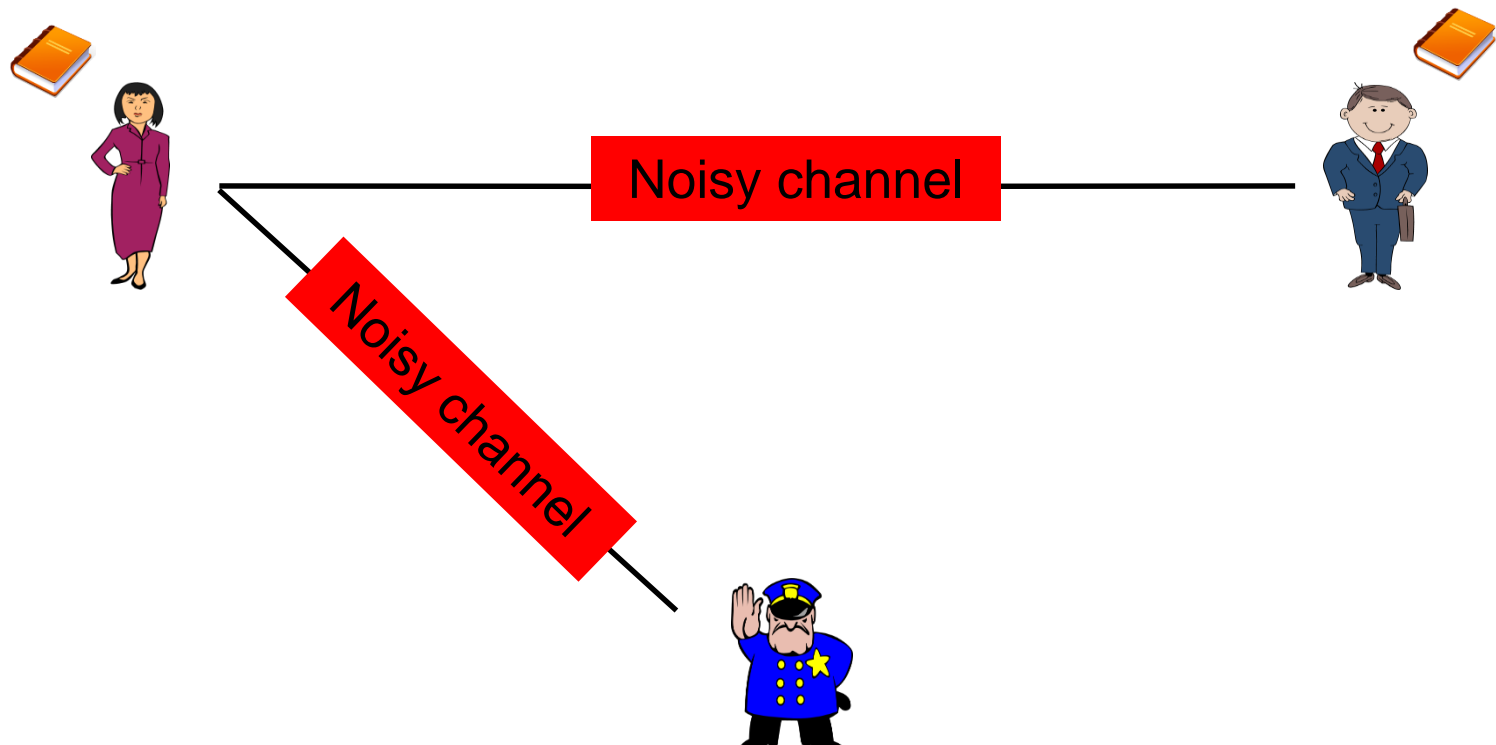
Covert Communication Model

- Alice has a noisy channel to Bob
- Alice and Bob prepare by sharing a secret



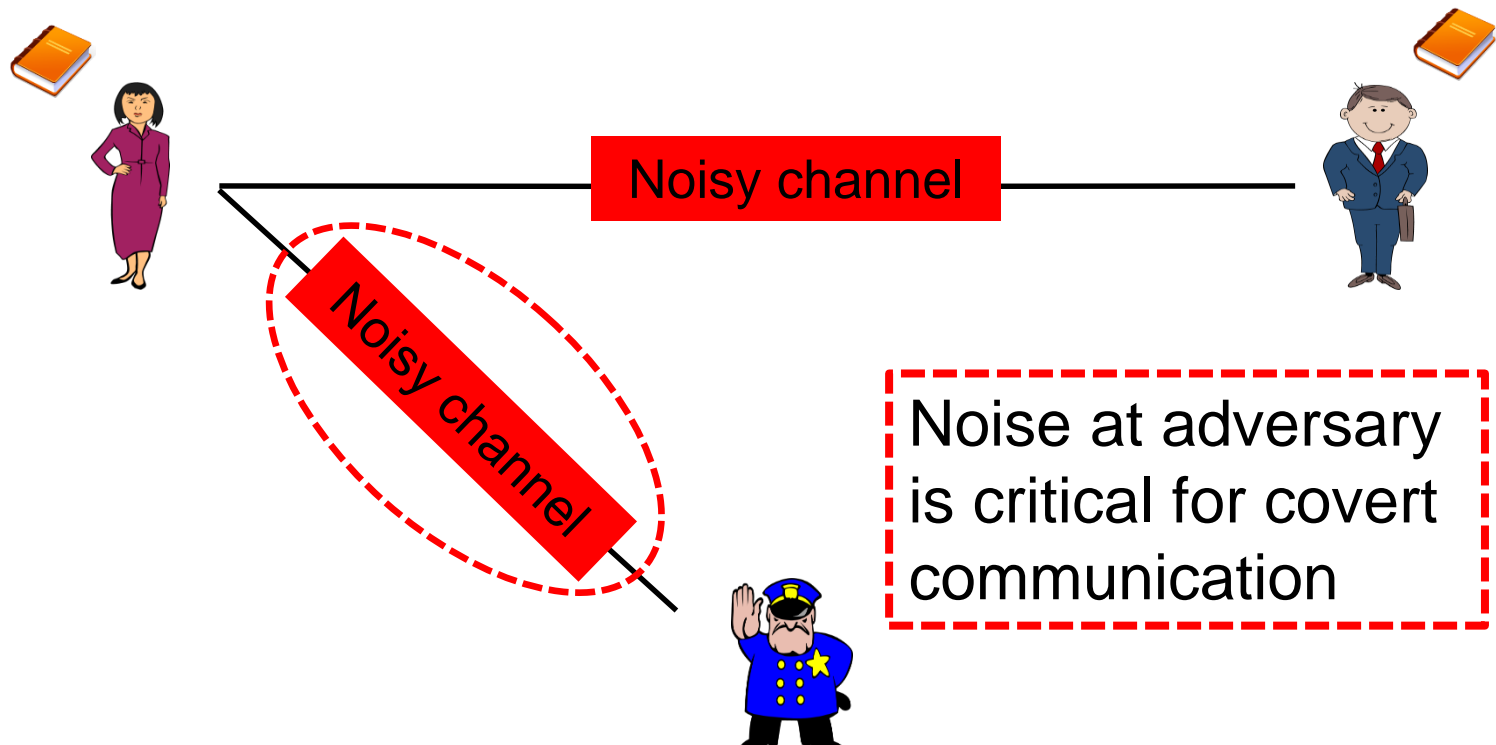
Covert Communication Model

- Alice has a noisy channel to Bob
- Alice and Bob prepare by sharing a secret
- Willie monitors his noisy channel from Alice for transmissions



Covert Communication Model

- Alice has a noisy channel to Bob
- Alice and Bob prepare by sharing a secret
- Willie monitors his noisy channel from Alice for transmissions



Hypothesis testing

- Willie attempts to classify observations of Alice's channel as either noise or signal corrupted by noise
 - Binary hypothesis test

		Willie decides he saw	
		Noise	Signal+Noise
Alice is	quiet		$\mathbb{P}(\text{false alarm})$
	transmitting	$\mathbb{P}(\text{miss})$	$\mathbb{P}(\text{true detection})$

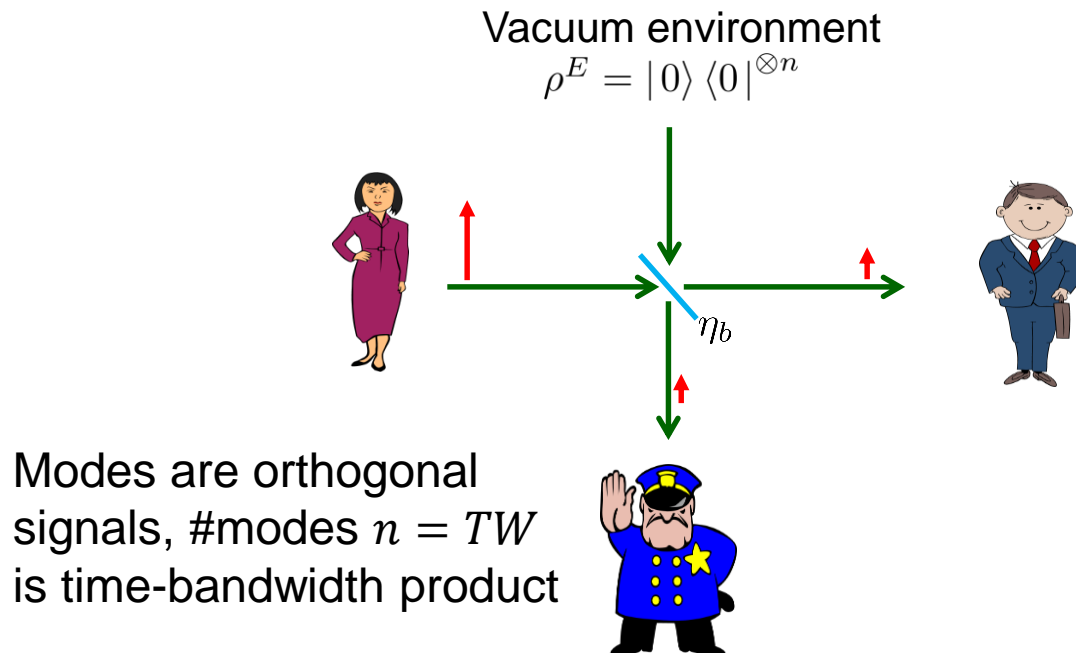
- Willie's probability of error $\mathbb{P}_e^{(w)} = \frac{\mathbb{P}(\text{miss}) + \mathbb{P}(\text{false alarm})}{2} \leq \frac{1}{2}$
- Alice desires $\mathbb{P}_e^{(w)} \geq \frac{1}{2} - \epsilon$ ← **“Coverttness” criterion**

Outline

- Introduction
- Preliminaries
- Analysis of covert optical communication
- Experimental results
- Conclusion: Vision for Shadow Network Architecture

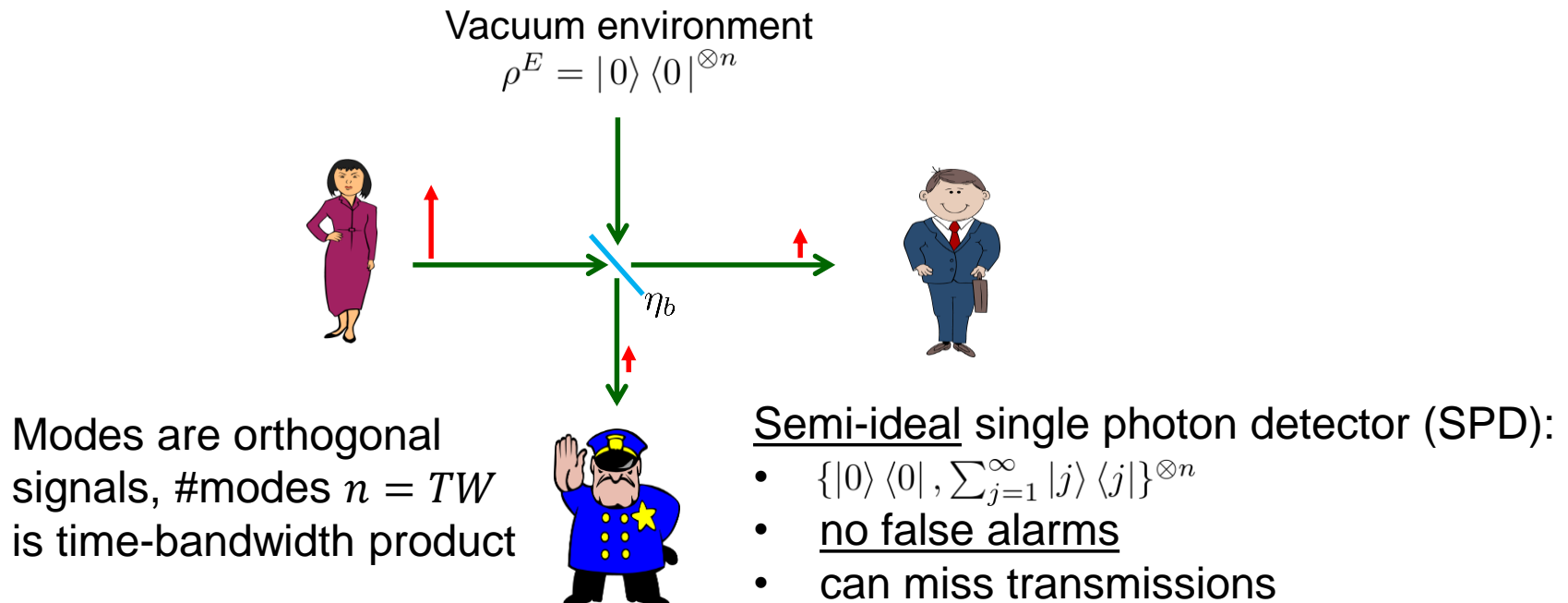
Noiseless measurements on pure-loss channel

- Bosonic channel is the quantum-mechanical description of an optical channel with linear loss (beam splitter)



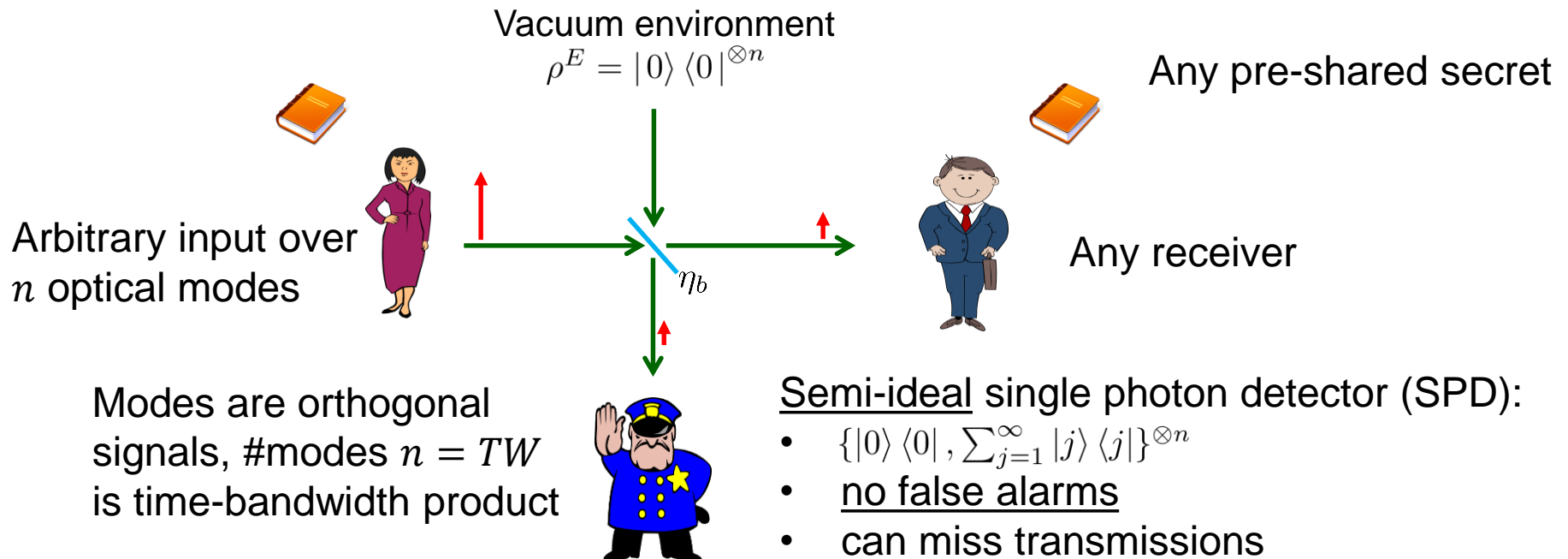
Noiseless measurements on pure-loss channel

- Bosonic channel is the quantum-mechanical description of an optical channel with linear loss (beam splitter)



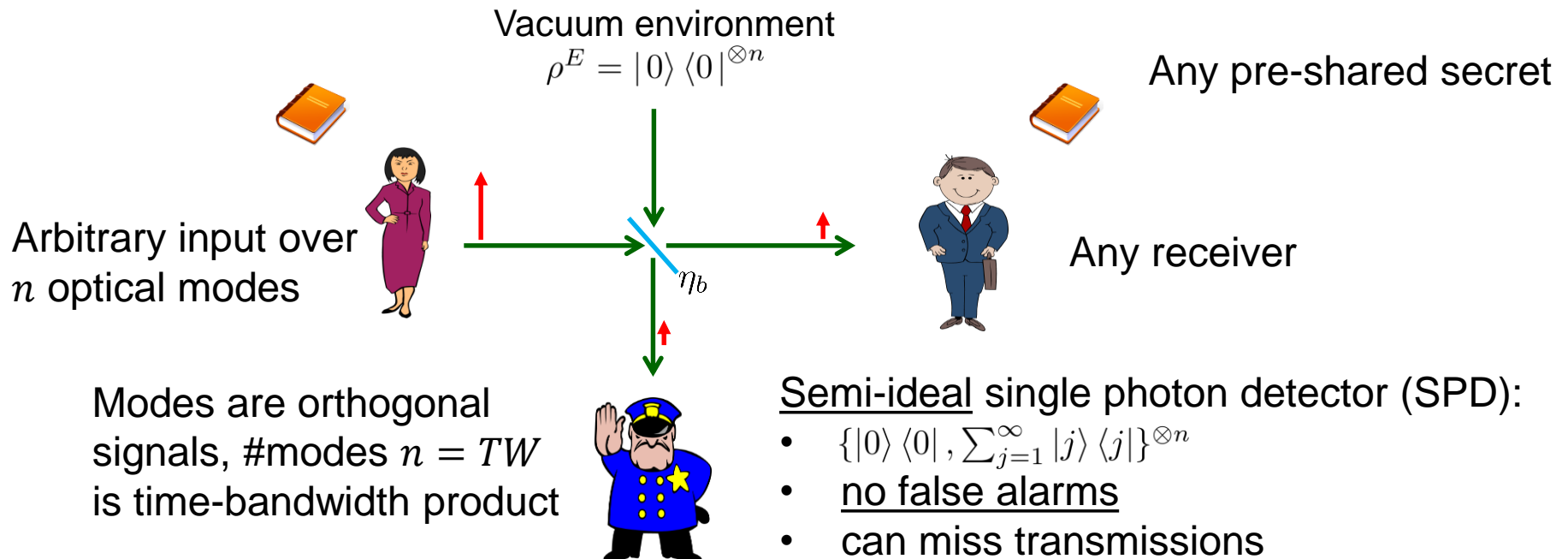
Noiseless measurements on pure-loss channel

- Bosonic channel is the quantum-mechanical description of an optical channel with linear loss (beam splitter)



Noiseless measurements on pure-loss channel

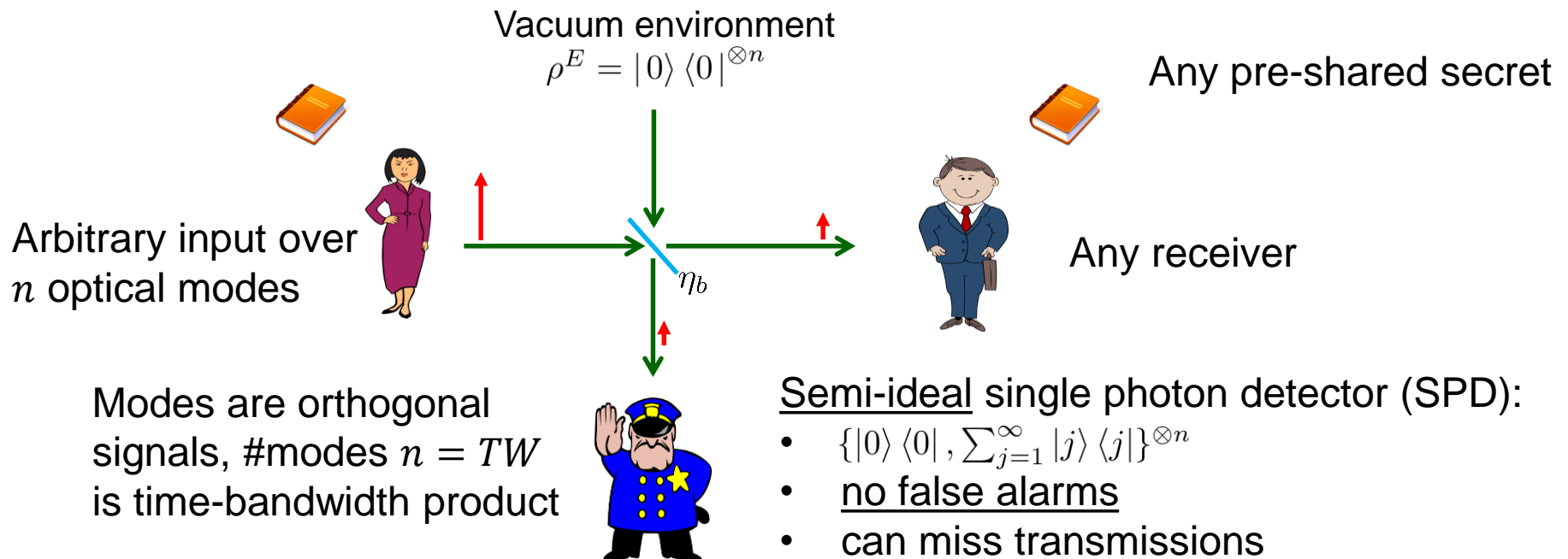
- Bosonic channel is the quantum-mechanical description of an optical channel with linear loss (beam splitter)



- No covert communication possible!

Noiseless measurements on pure-loss channel

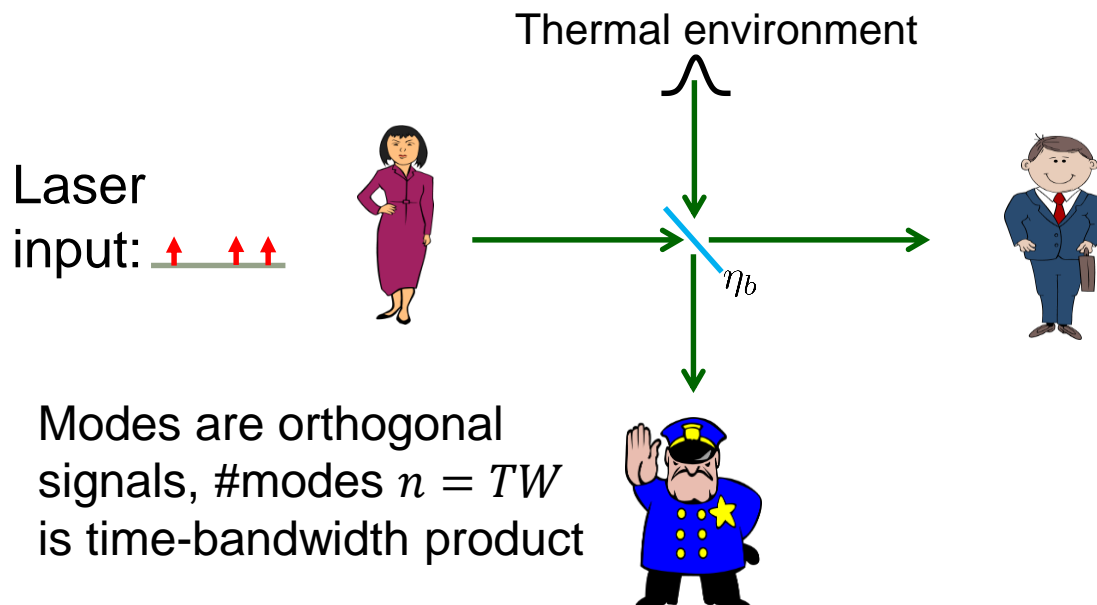
- Bosonic channel is the quantum-mechanical description of an optical channel with linear loss (beam splitter)



- No covert communication possible!
- Conditions unlikely to ever occur practically
 - Noisy environment (Planck's Law), non-ideal detectors

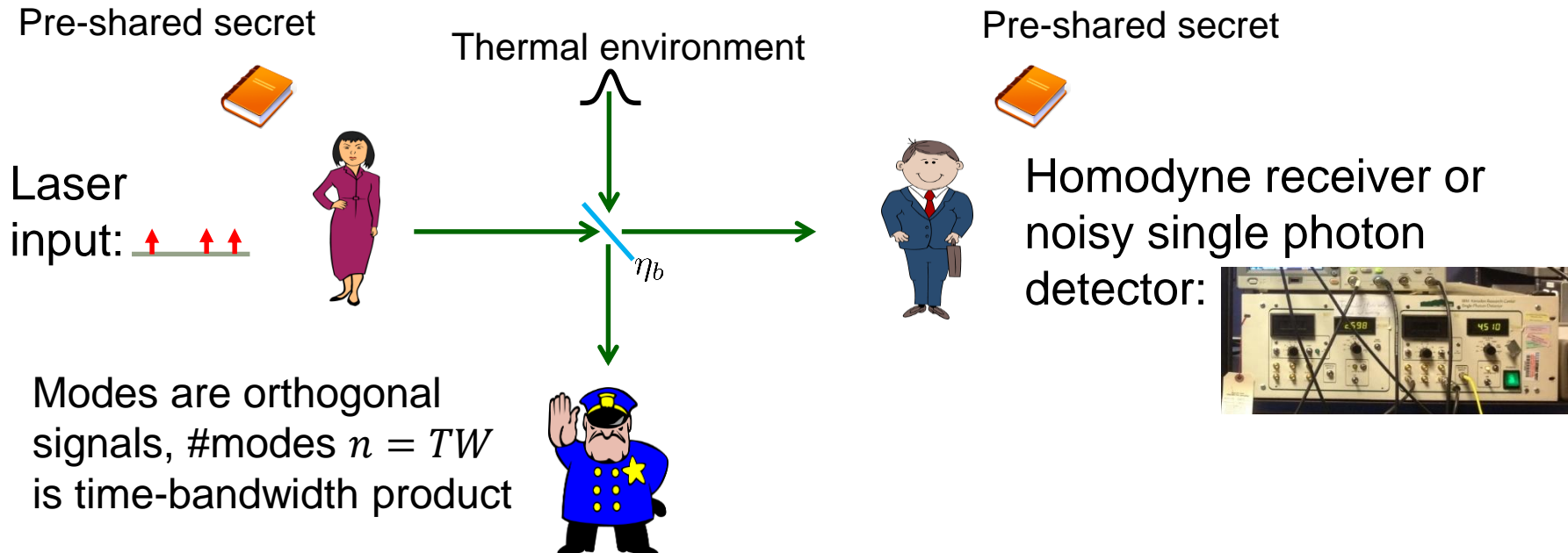
Thermal noise channel

- Beamsplitter models the optical channel



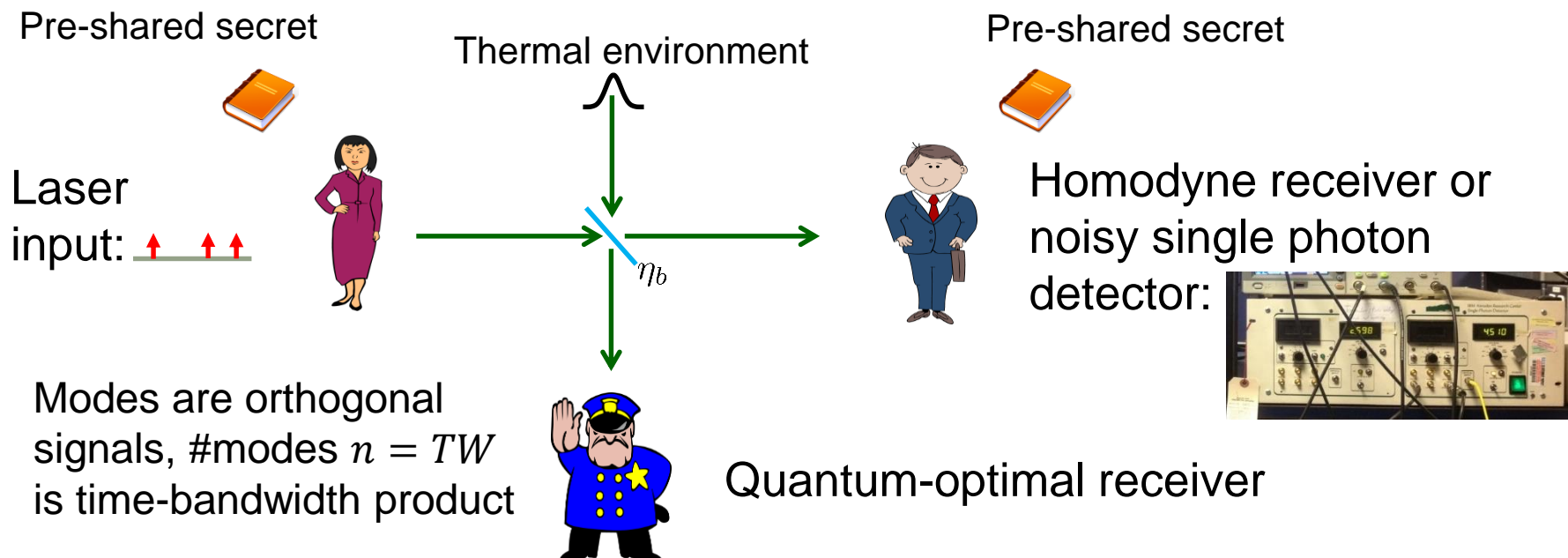
Thermal noise channel

- Beamsplitter models the optical channel



Thermal noise channel

- Beamsplitter models the optical channel



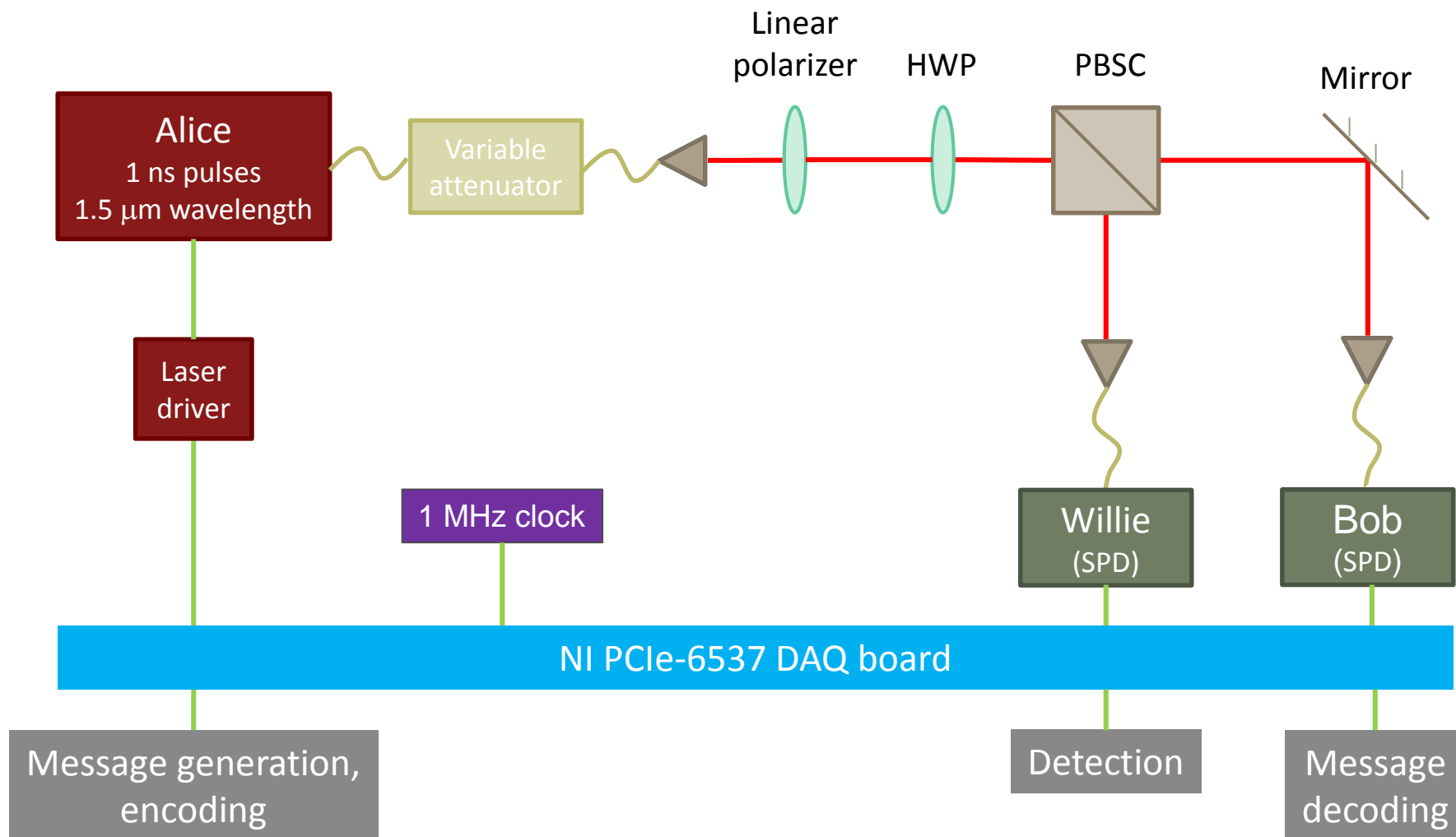
- Square root law: Alice can reliably transmit $O(\sqrt{n})$ covert bits using n optical modes, and no more

– Mean photon number (power) per mode $\langle N_S \rangle = O\left(\frac{1}{\sqrt{n}}\right)$ photons to hide in the noise

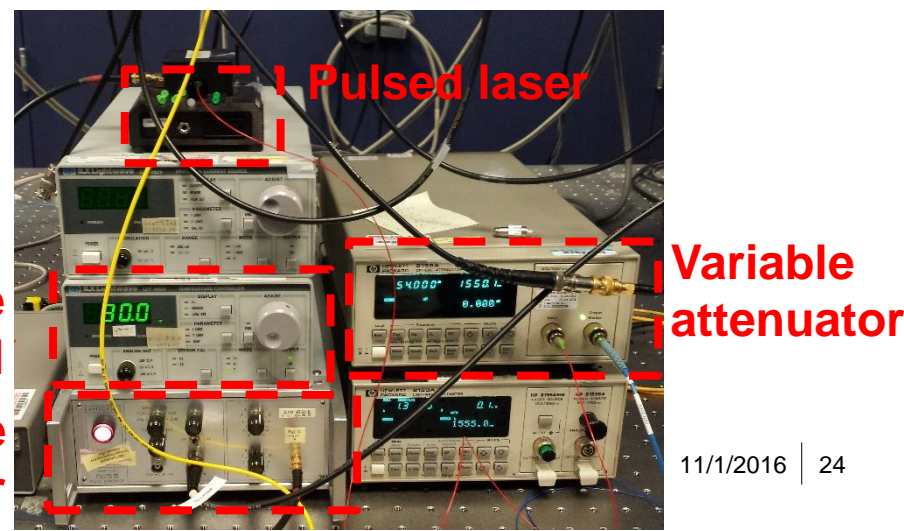
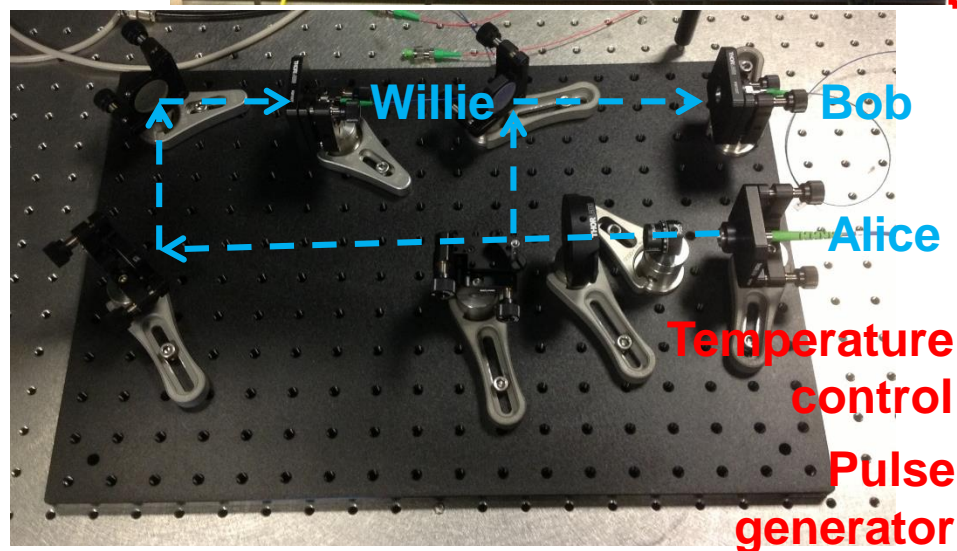
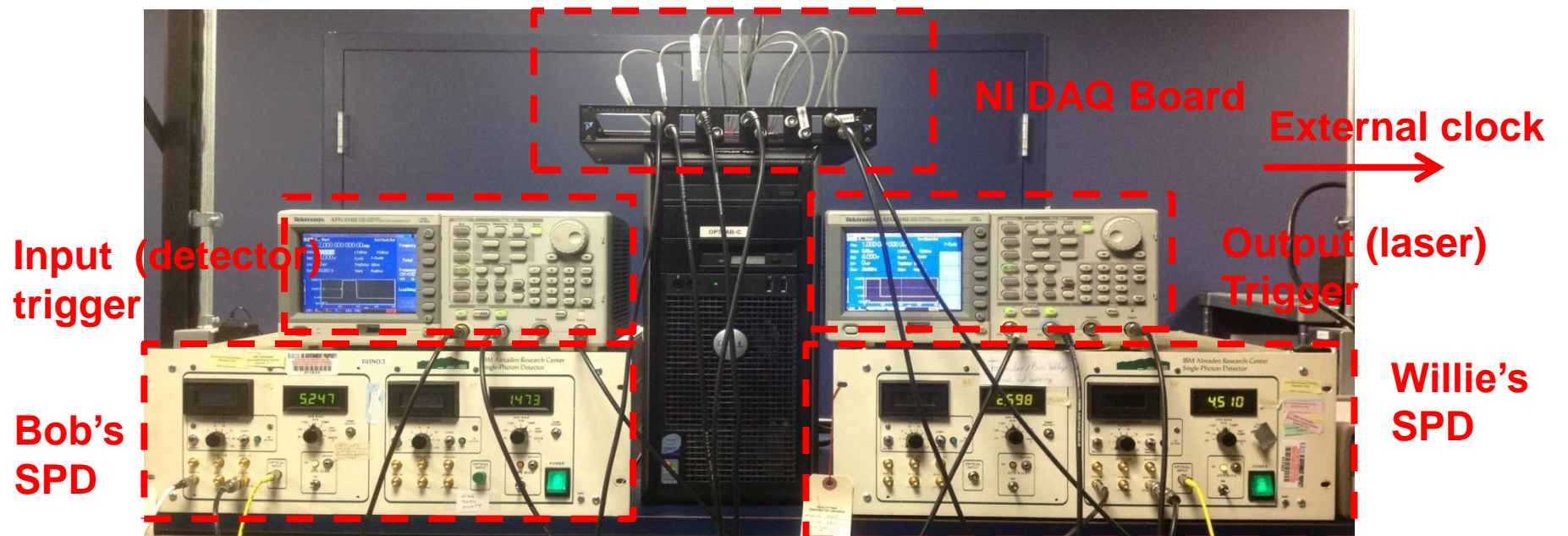
Outline

- Introduction
- Preliminaries
- Analysis of covert optical communication
- Experimental results
- Conclusion: Vision for Shadow Network Architecture

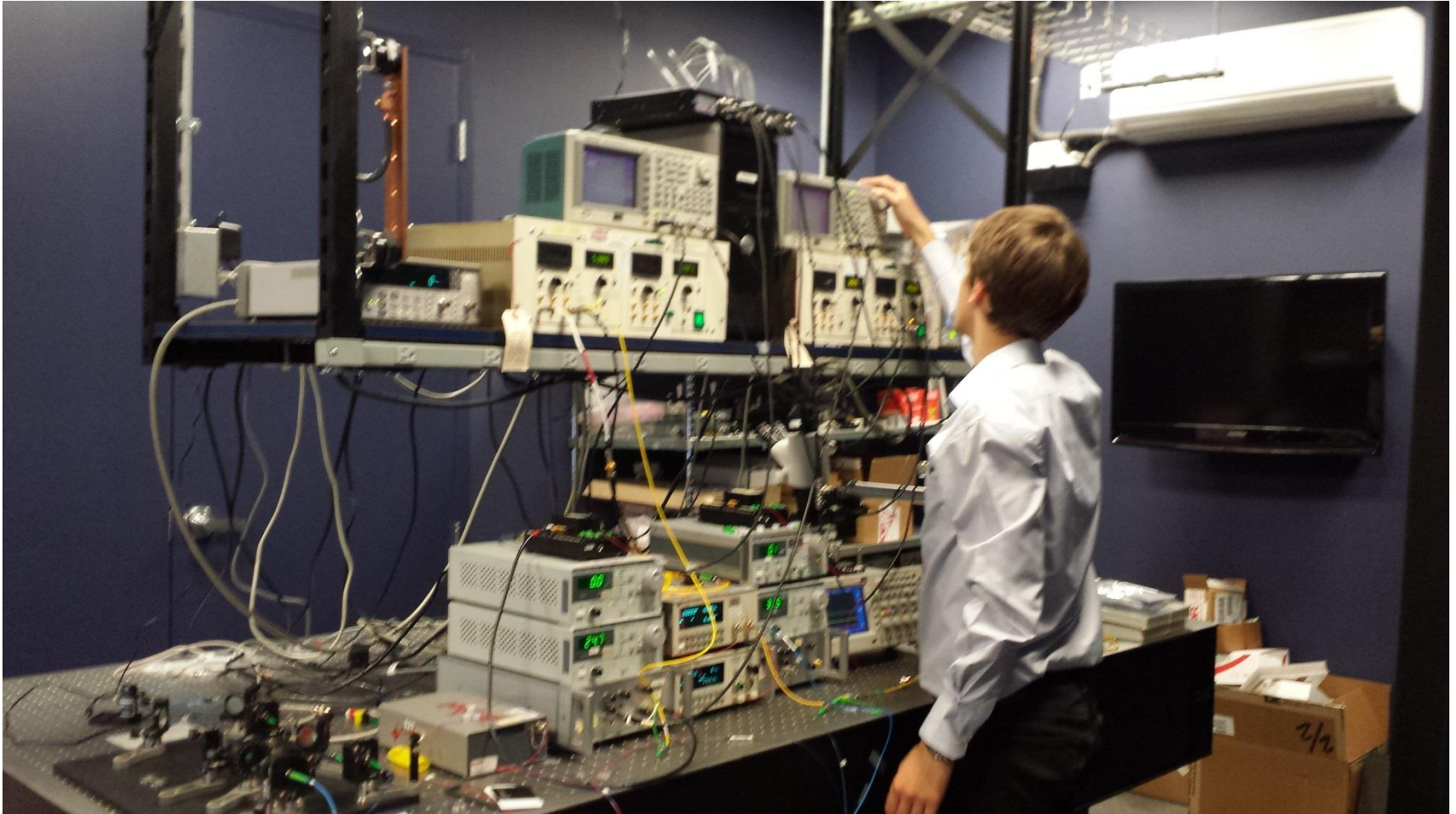
Experimental setup



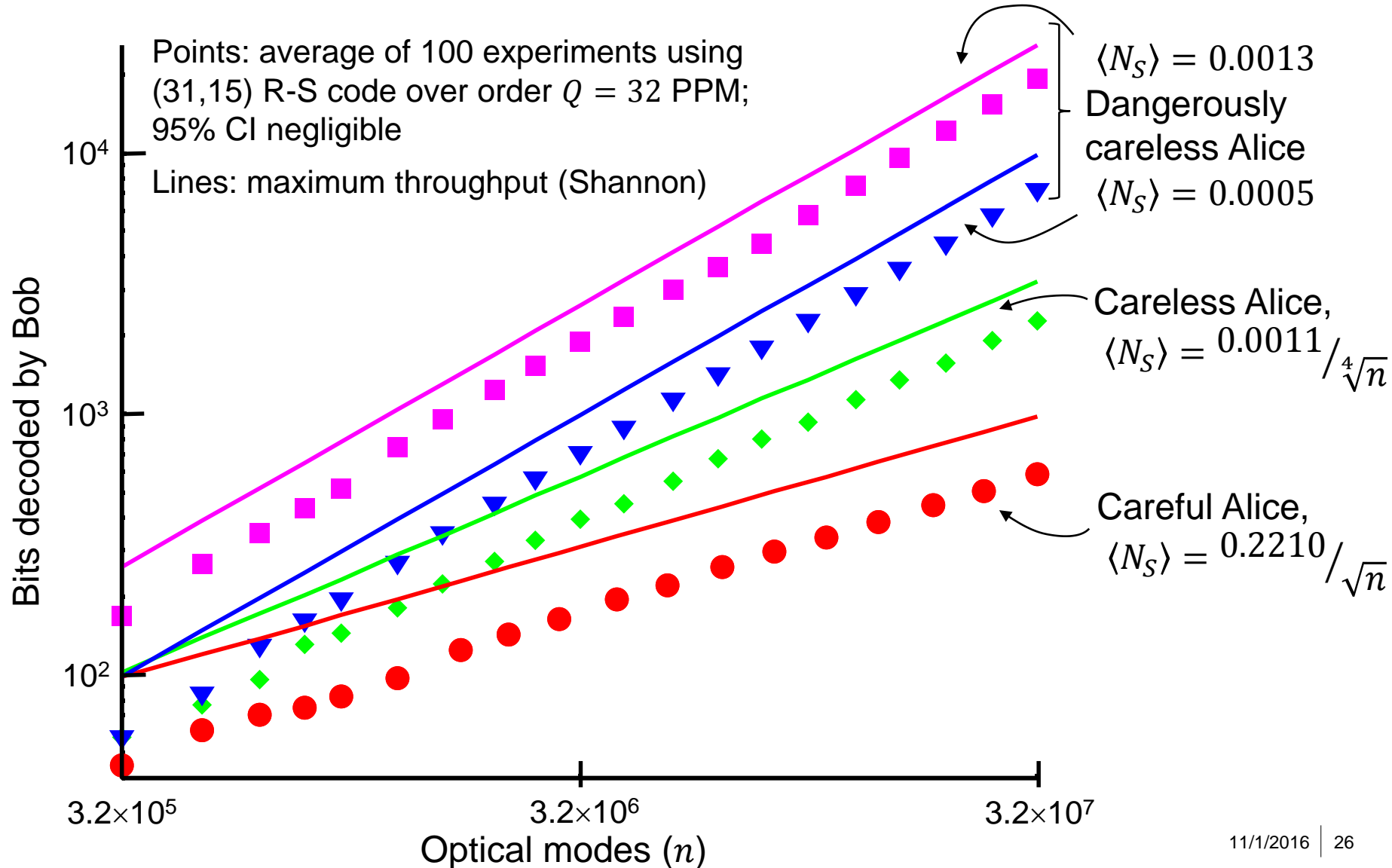
Experimental setup



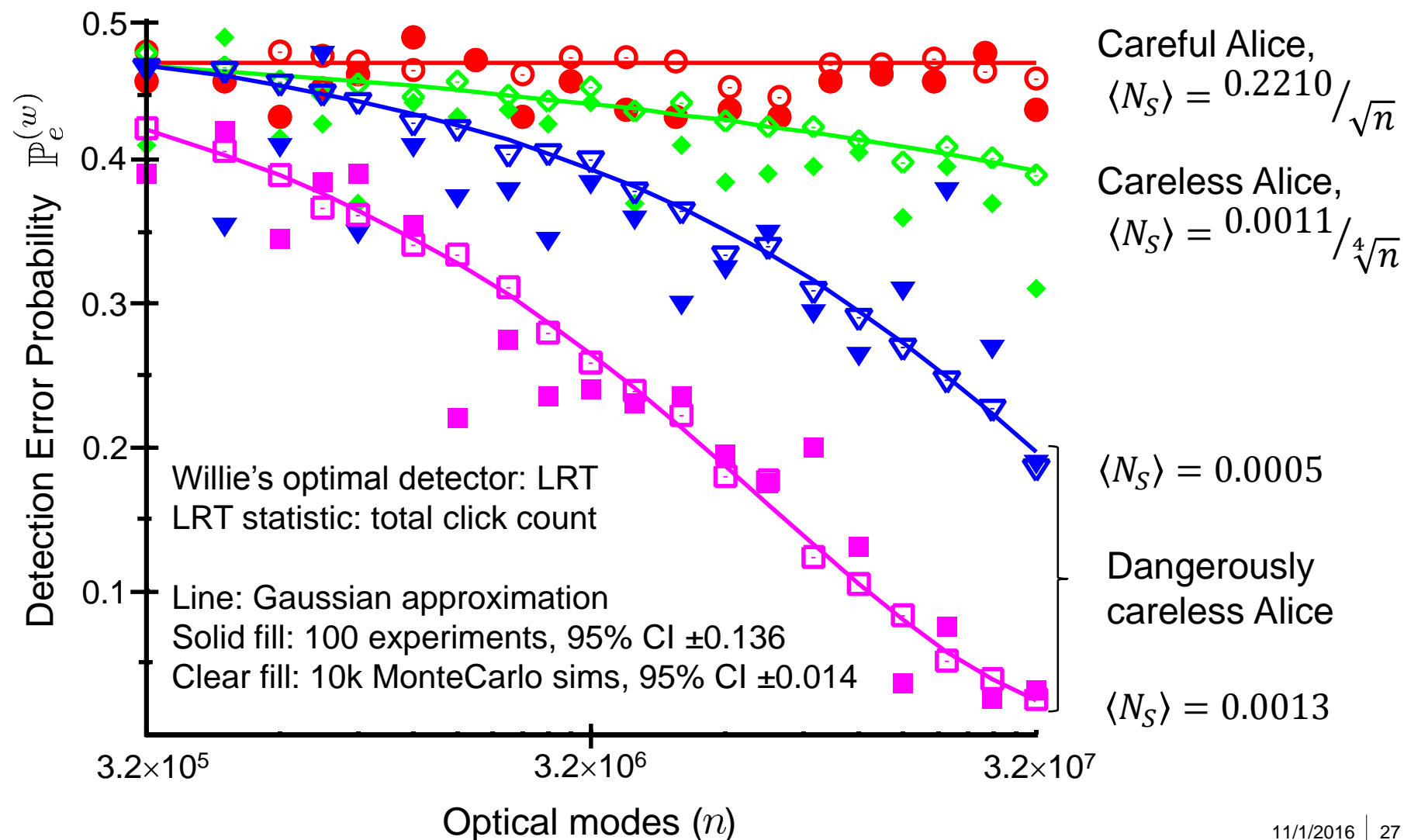
Experimental setup



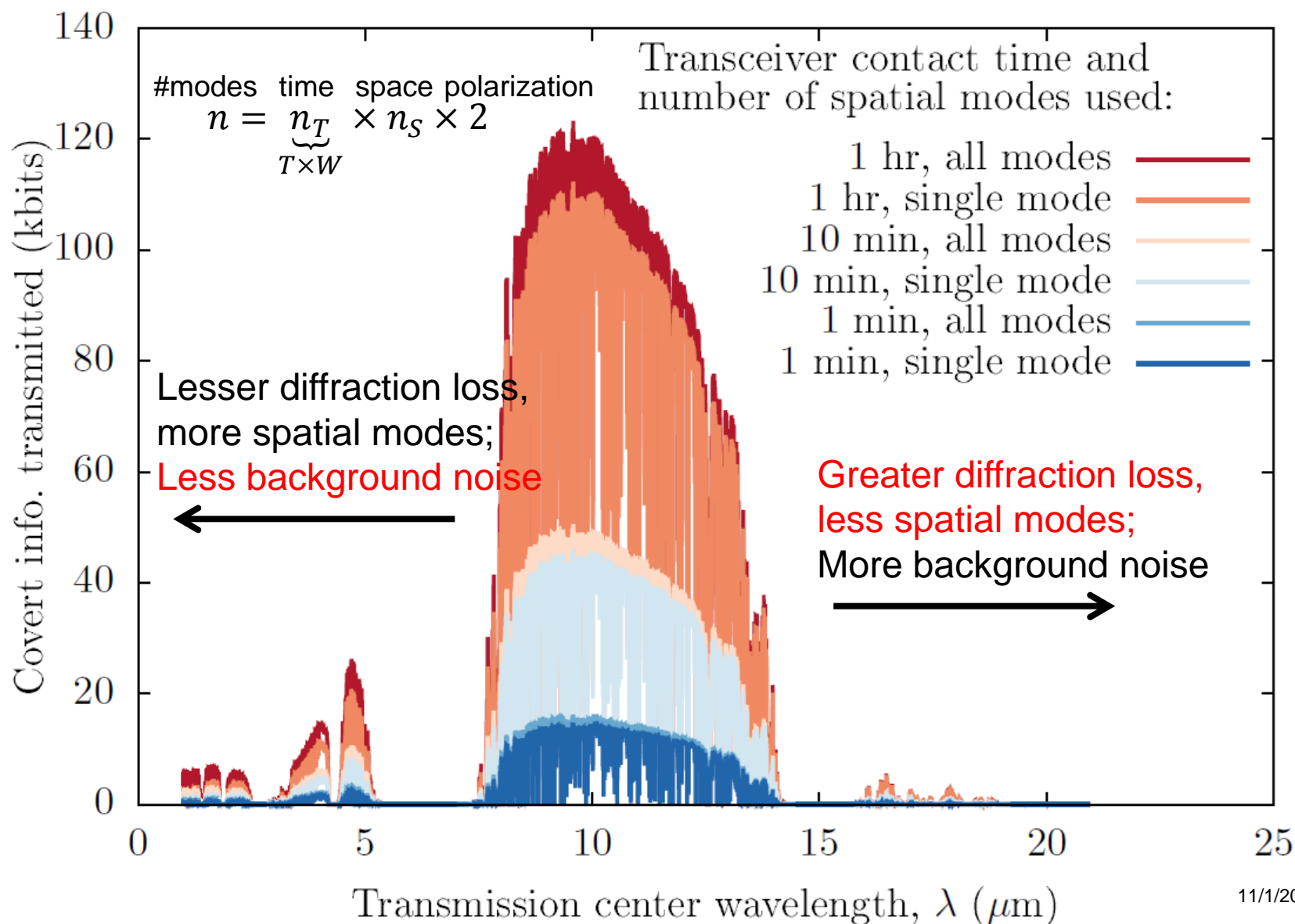
Number of bits received by Bob



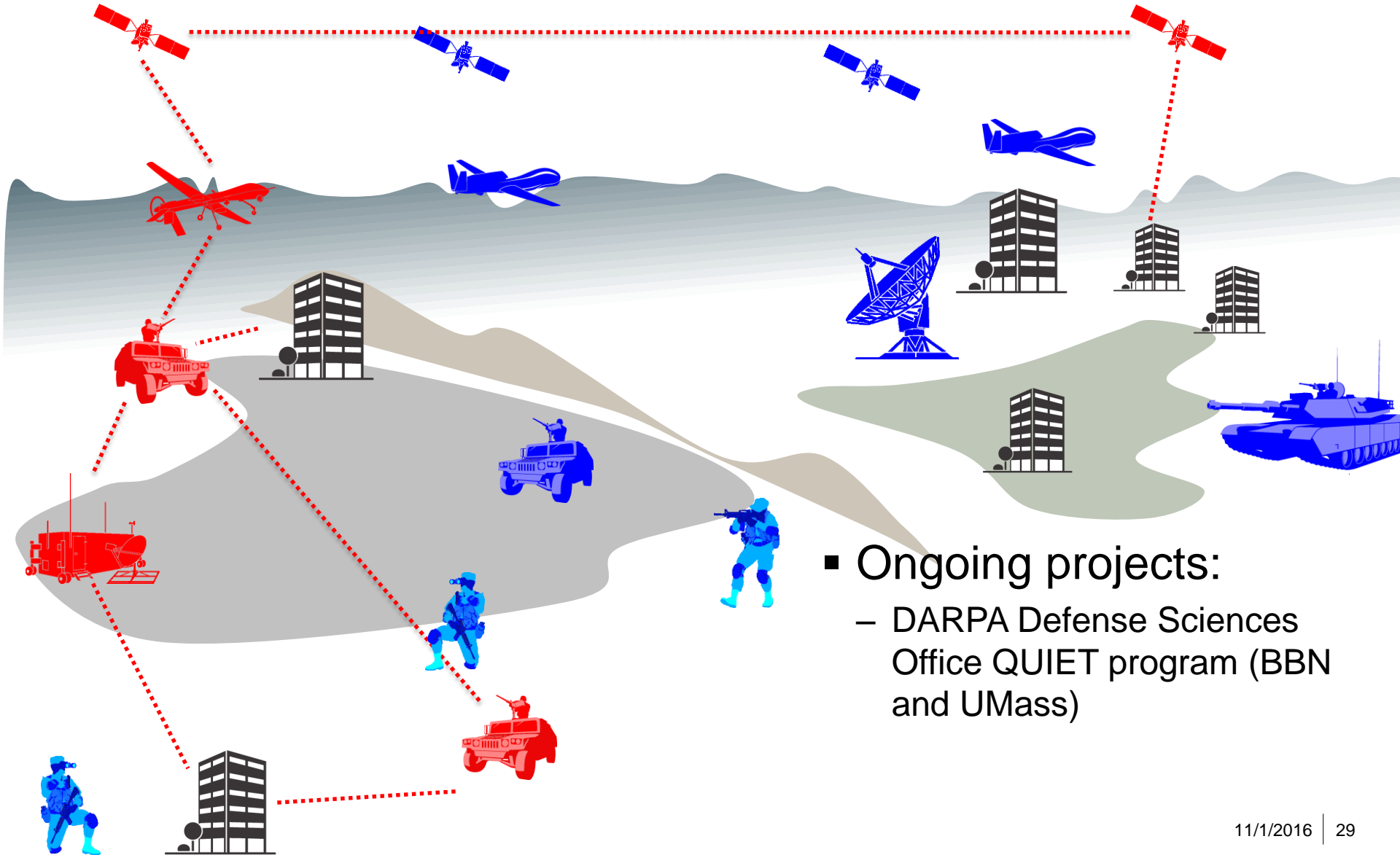
Willie detection error probability



What is the optimal center bandwidth?

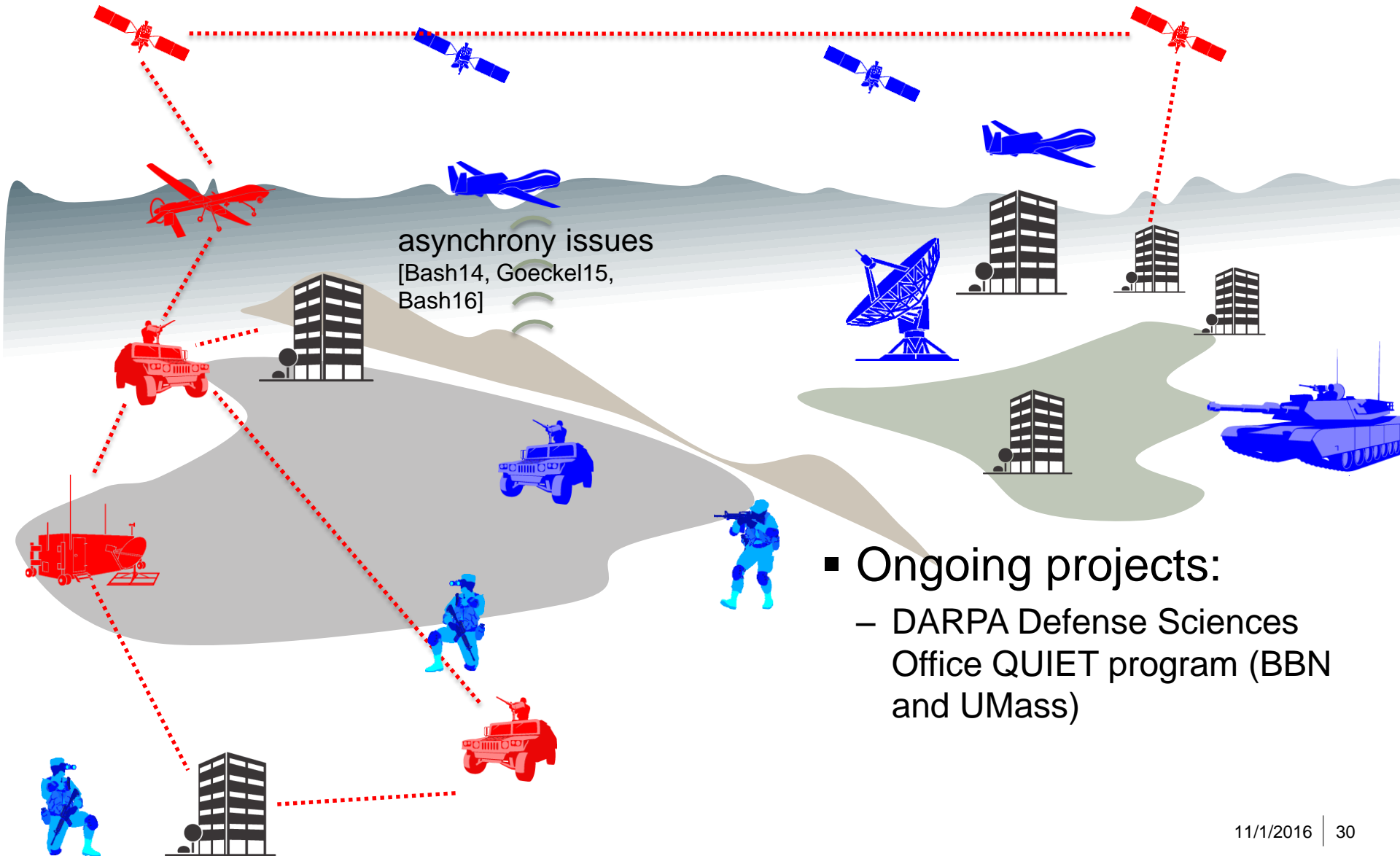


Conclusion: Vision for Shadow Network Architecture

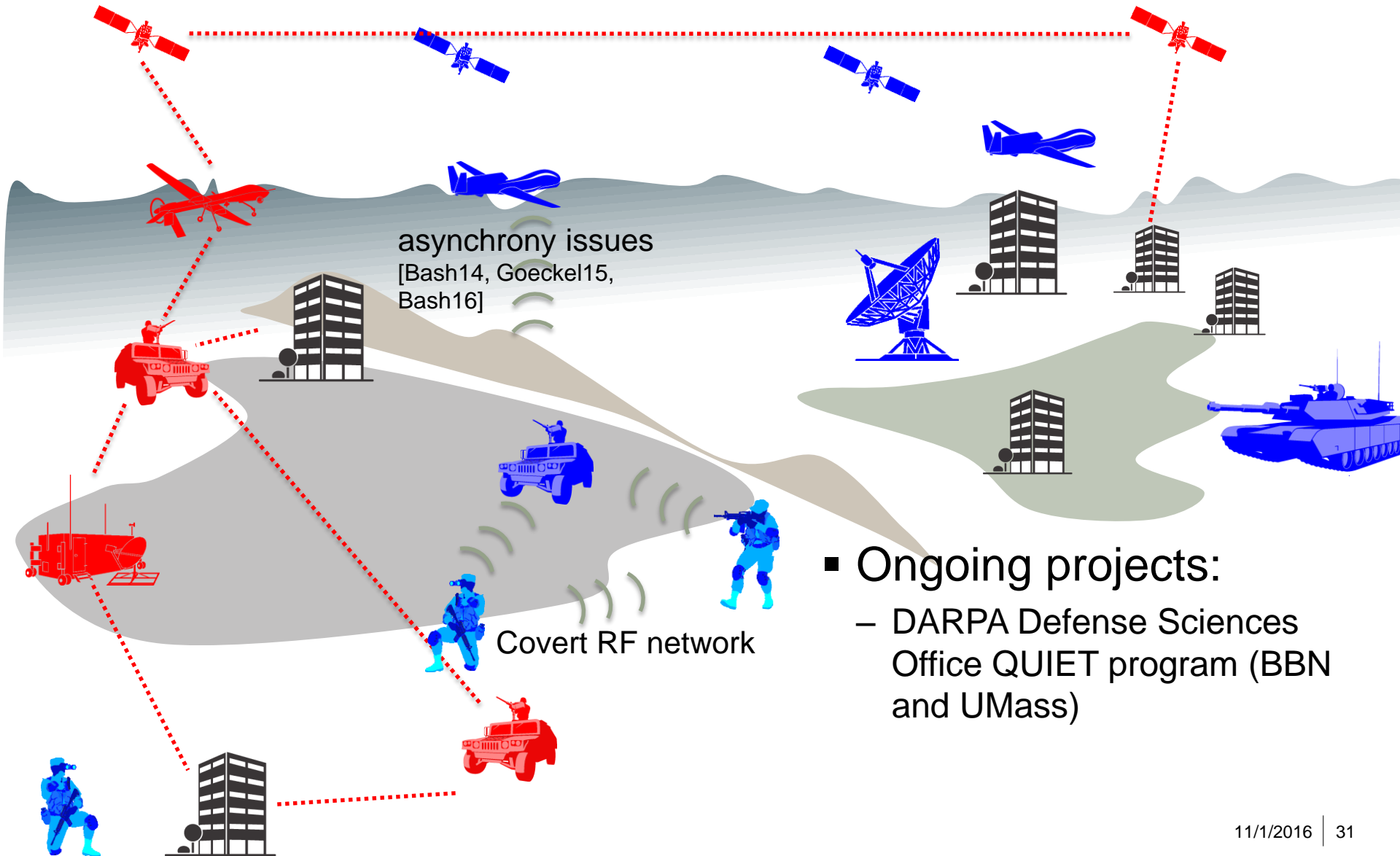


- Ongoing projects:
 - DARPA Defense Sciences Office QUIET program (BBN and UMass)

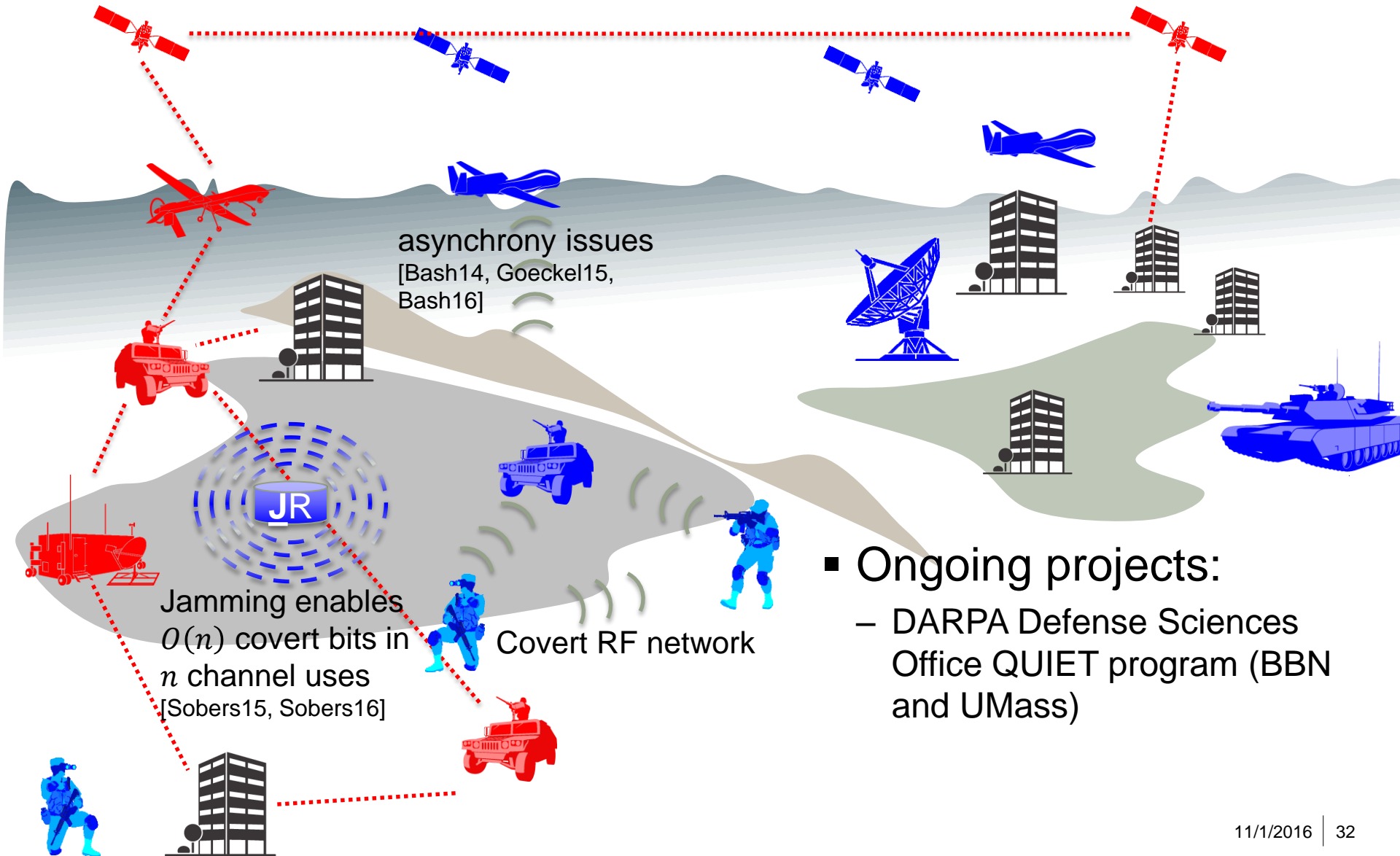
Conclusion: Vision for Shadow Network Architecture



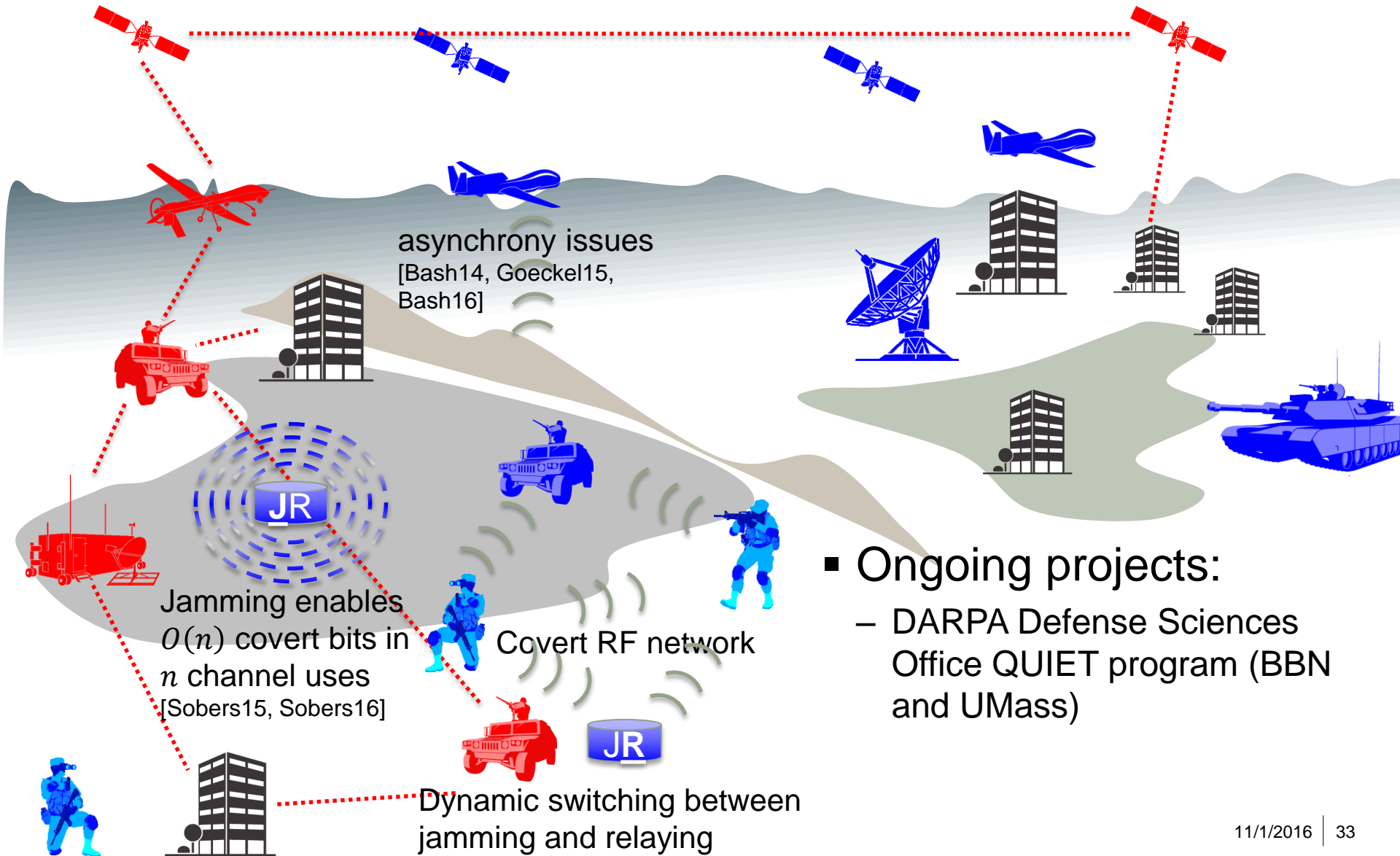
Conclusion: Vision for Shadow Network Architecture



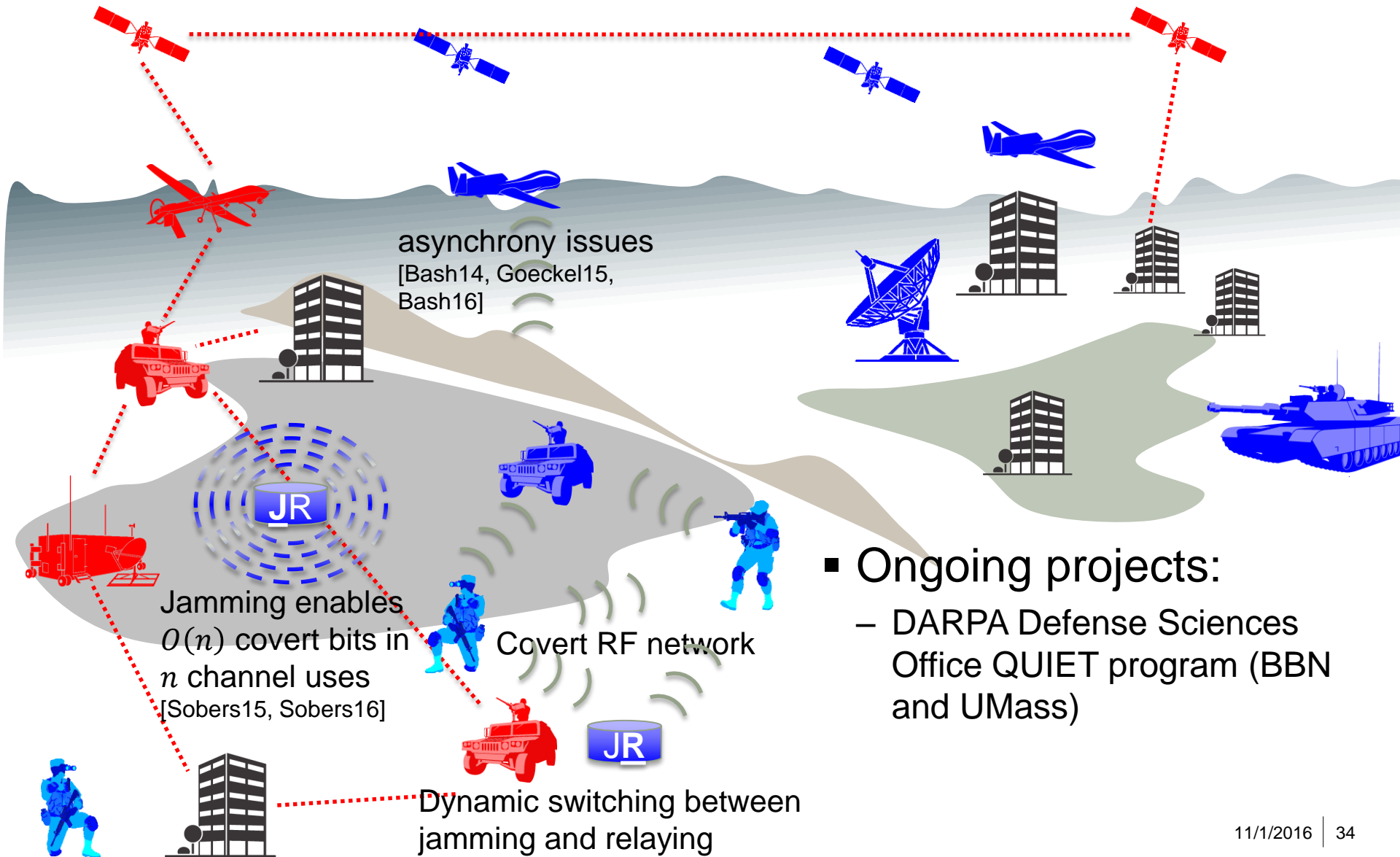
Conclusion: Vision for Shadow Network Architecture



Conclusion: Vision for Shadow Network Architecture

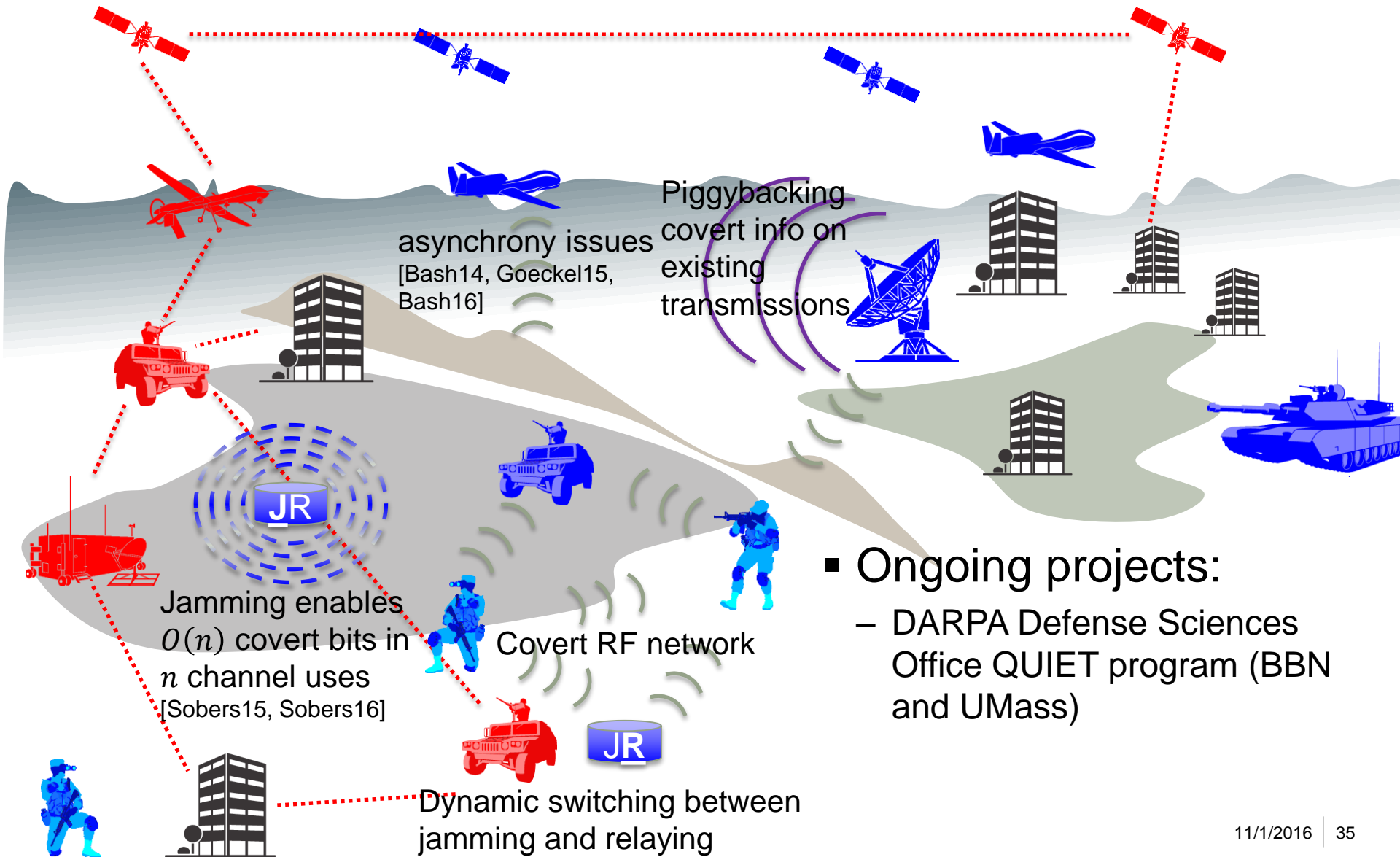


Conclusion: Vision for Shadow Network Architecture

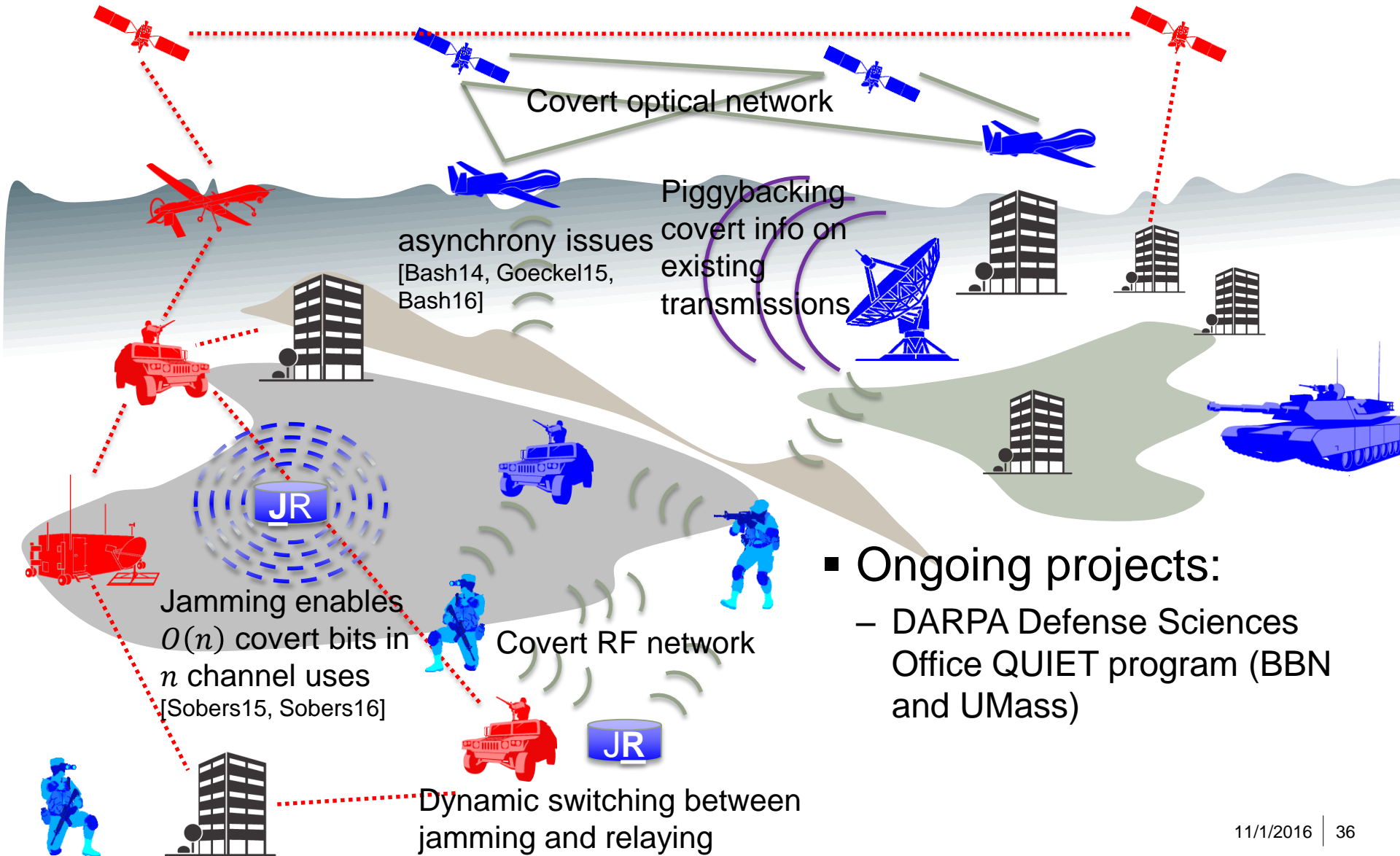


- Ongoing projects:
 - DARPA Defense Sciences Office QUIET program (BBN and UMass)

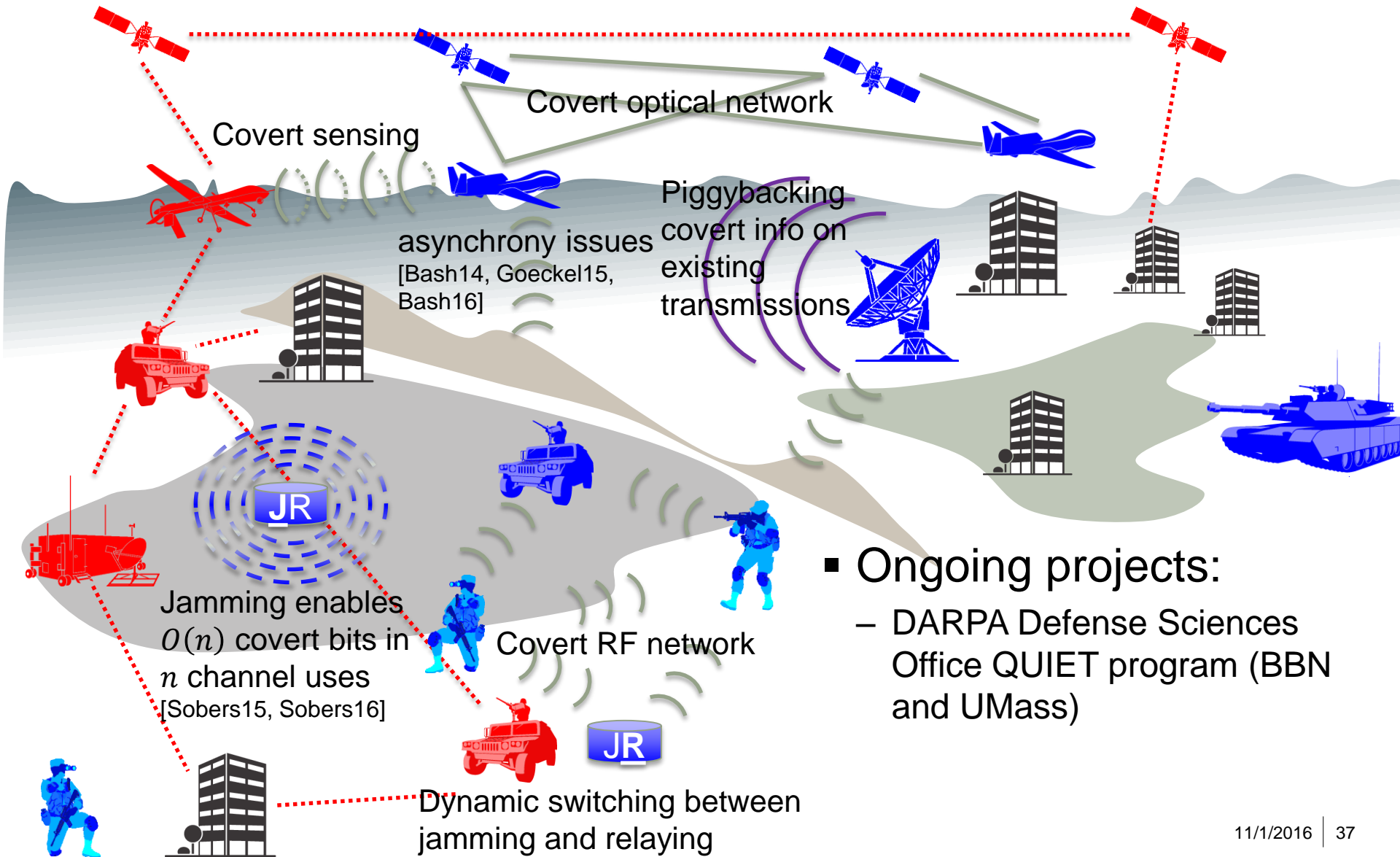
Conclusion: Vision for Shadow Network Architecture



Conclusion: Vision for Shadow Network Architecture

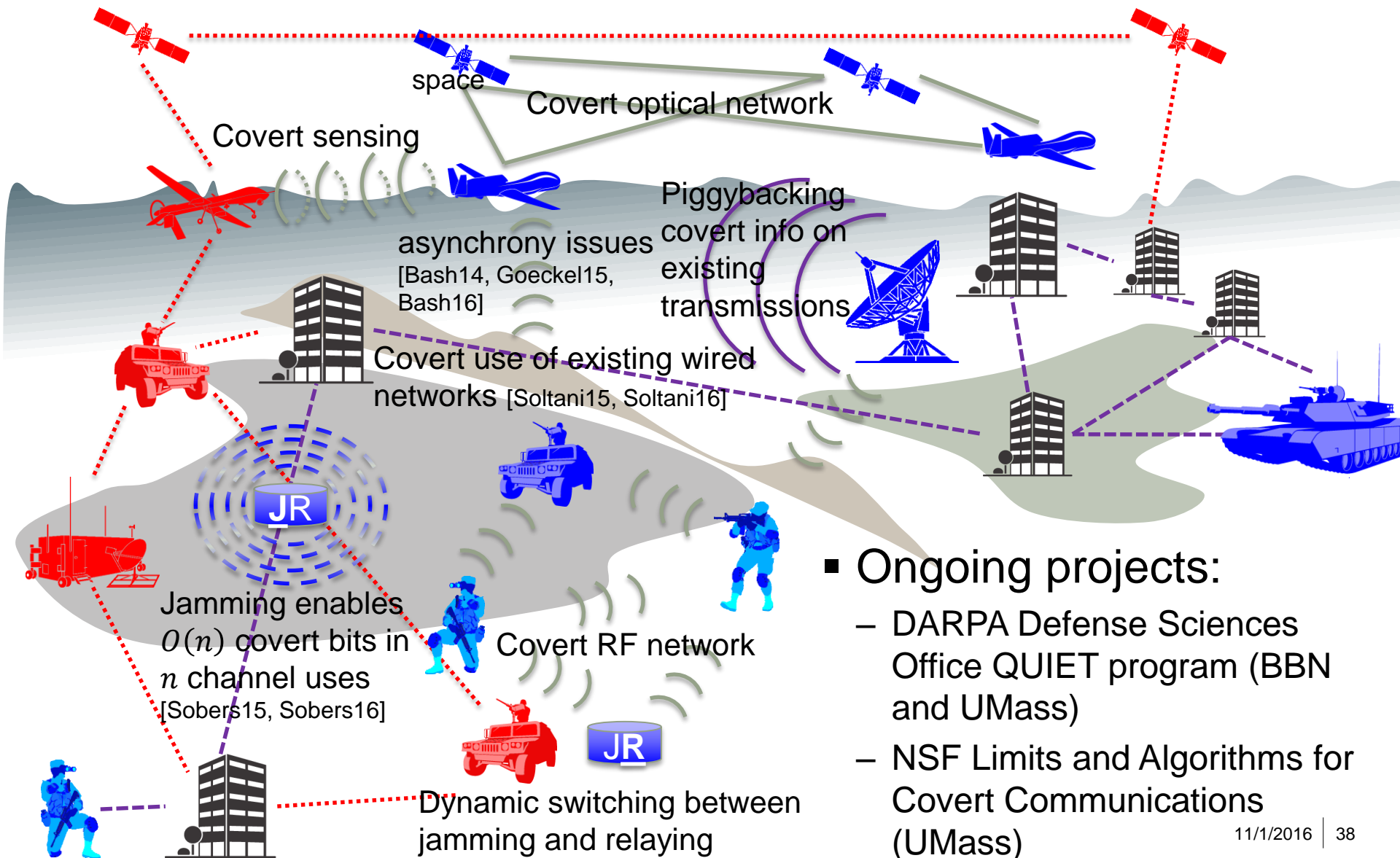


Conclusion: Vision for Shadow Network Architecture



- Ongoing projects:
 - DARPA Defense Sciences Office QUIET program (BBN and UMass)

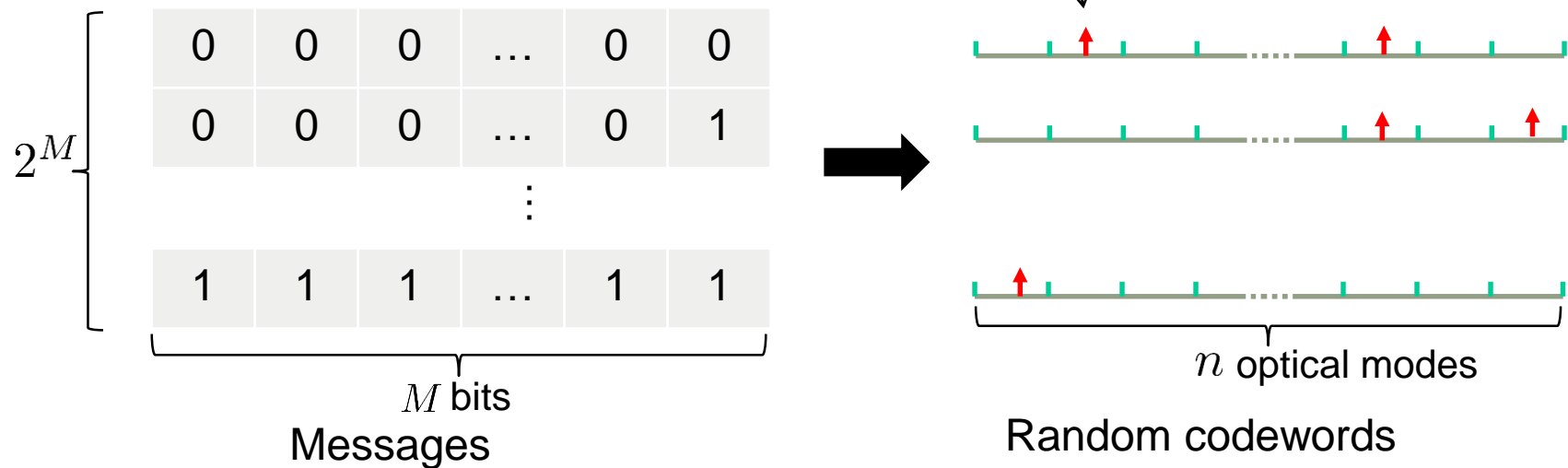
Conclusion: Vision for Shadow Network Architecture



Backup slides

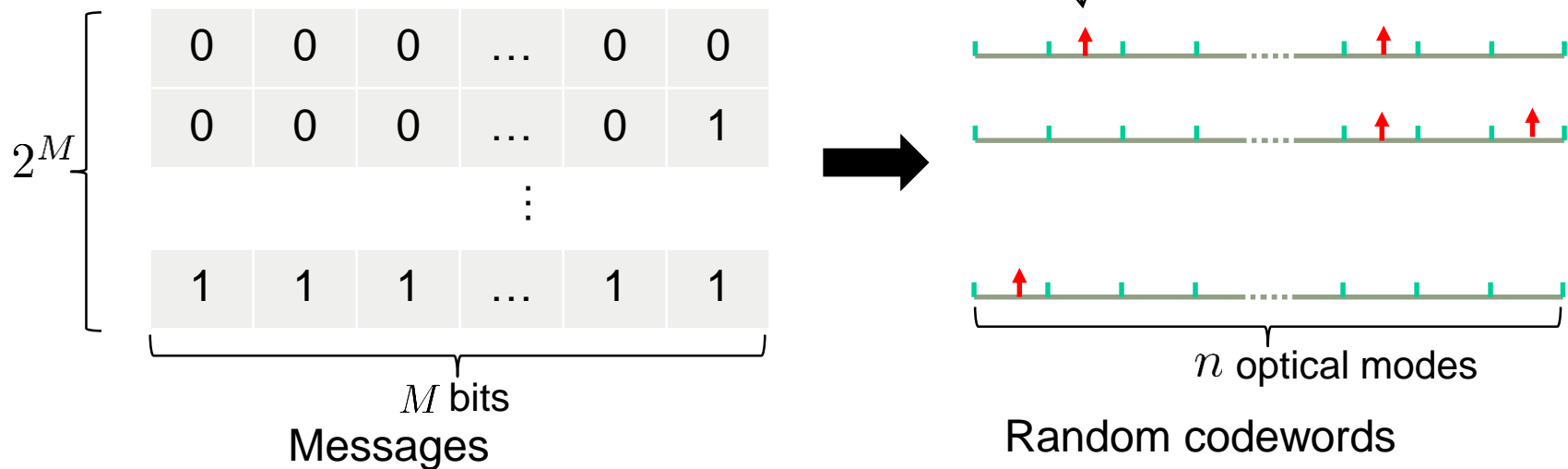
Proof construction for practical receivers

- On-off keying modulation, random code, ML decode
 - Probability of “on” pulse $p_{\text{on}} = \mathcal{O}(1/\sqrt{n})$ ensures stealth with secret codebook



Proof construction for practical receivers

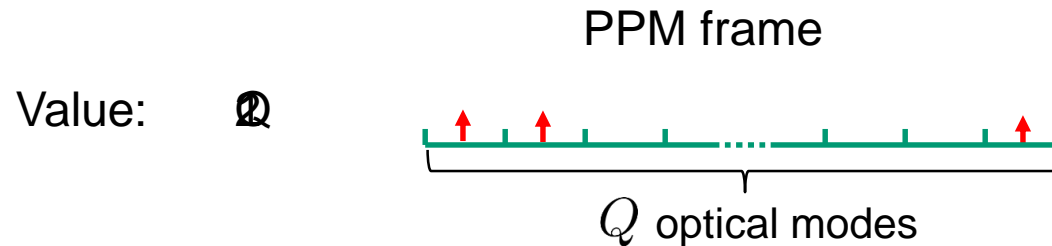
- On-off keying modulation, random code, ML decode
 - Probability of “on” pulse $p_{\text{on}} = \mathcal{O}(1/\sqrt{n})$ ensures stealth with secret codebook



- Easy analysis but implementation impractical
 - Desire to use structured, public error correction code (ECC)

Pulse-position modulation (PPM) signaling

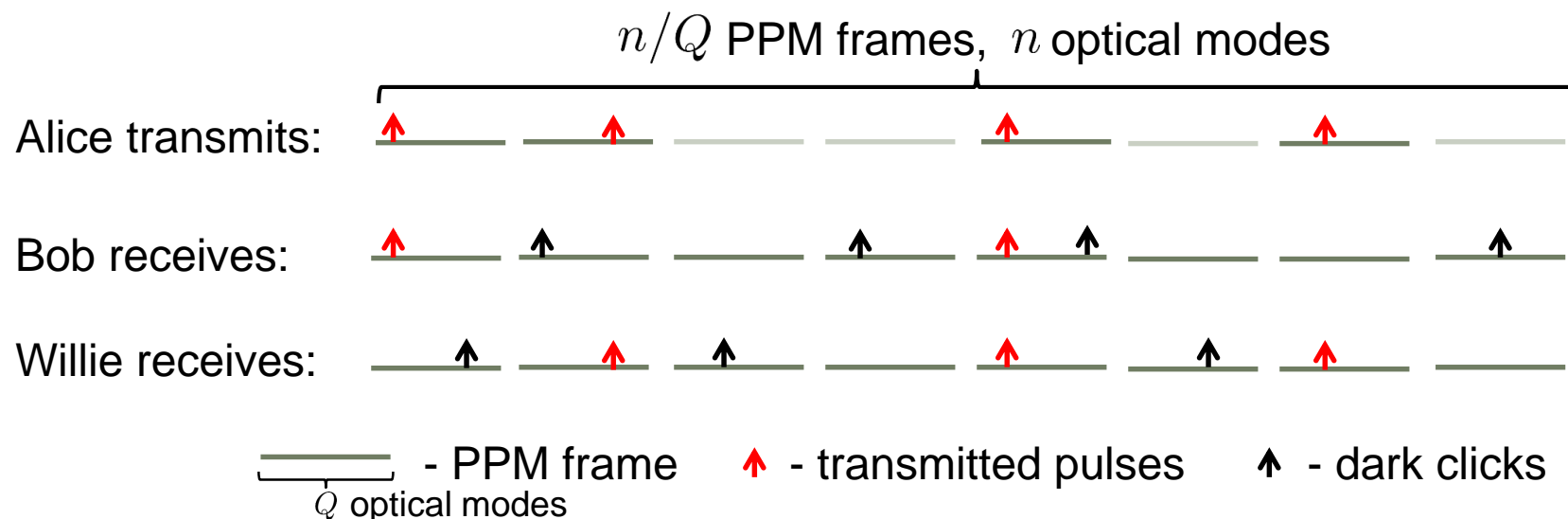
- Pulse-position modulation (PPM) signaling uses pulse location to encode value:



- Then use an outer ECC on top of PPM
- Challenge for covert communication: every PPM symbol requires a pulse, zero pulses not allowed

Using PPM Alphabet

- Solution: given n/Q possible PPM frames, Alice and Bob secretly agree on a random subset \mathcal{S} to use for message transmission, $\mathbb{E}[|\mathcal{S}|] = \mathcal{O}(\sqrt{n/Q})$



- Bob ignores the “empty” frames, but Willie cannot since he doesn’t know where they are

Covert communication with PPM

- Alice and Bob also construct vector $\mathbf{k} = [k_1, \dots, k_{|\mathcal{S}|}]$ secretly, with each k_i chosen uniformly at random from $\{0, 1, \dots, Q - 1\}$
- Alice transmits $(\mathbf{c}(W) + \mathbf{k}) \bmod Q$ using frames in \mathcal{S}

Codebook \mathcal{S} $\mathbf{c}(W)$ 

- Bob subtracts \mathbf{k} modulo Q , then decodes
- Willie cannot exploit ECC structure
- SRL: Alice can reliably transmit $\mathcal{O}(\sqrt{n/Q} \log Q)$ covert bits in n optical channel uses with public random code
- However, we use Reed-Solomon for experiments

Experimental design


■ Data

- 100 testbed experiments per data point
- 10k Monte-Carlo simulations per data point (Willie only)
 - Simulate optical channel induced by laser-light transmitter and SPD using measured testbed characteristics

■ Bob

- $Q = 32$ PPM, (31,15) Reed-Solomon ECC
- Report average number of decoded bits
- Observed characteristics \Rightarrow max throughput from Shannon capacity

■ Willie

- Optimal detector = LRT
- Estimate  from empirical distributions of LRT statistics
- LRT statistic \approx total click count \Rightarrow Gaussian approximation

References (1)

- Spread spectrum technology references:
 - [Simon94] Simon et al., “Spread Spectrum Communications Handbook,” McGraw Hill, New York, NY (1994).
 - [Nicholson88] D.L. Nicholson, “Spread Spectrum Signal Design: LPE and AJ Systems,” Computer Science Press, Rockville, MD (1988)
- Our work on covert communication:
 - [Bash12] **B. A. Bash[†]**, D. Goeckel, and D. Towsley, “Square Root Law for Communication with Low Probability of Detection on AWGN Channels,” Proc. IEEE Int. Symp. Inf. Theory (ISIT), Cambridge, MA (2012)
 - [Bash13a] **B. A. Bash[†]**, D. Goeckel, and D. Towsley, “Limits of reliable communication with low probability of detection on AWGN channels,” IEEE J. Sel. Areas Commun. **31** (9), 1921-1930 (2013).
 - [Bash13b] **B.A. Bash[†]**, **S. Guha[†]**, D. Goeckel, and D. Towsley, “Quantum Noise Limited Optical Communication with Low Probability of Detection,” Proc. IEEE Int. Symp. Inf. Theory (ISIT), Istanbul, Turkey (2013)
 - [Bash14] **B. A. Bash[†]**, D. Goeckel, and D. Towsley, “LPD Communication when the Warden Does Not Know When,” Proc. IEEE Int. Symp. Inf. Theory (ISIT), Honolulu, Hawaii (2014).

References (2)

- Our work on covert communication (continued):
 - [Soltani14] R. Soltani, **B. A. Bash**[†], D. Goeckel, **S. Guha**[†], and D. Towsley, “Artificial Noise Generation to Enhance LPD Throughput on AWGN Channels” Proc. Conf. on Commun., Control, Comp. (Allerton), Monticello, IL (2014)
 - [Bash15a] **B. A. Bash**[†], “Fundamental Limits of Covert Communication,” Ph.D. Thesis, University of Massachusetts, Amherst (2015)
 - [Bash15b] **B. A. Bash**[†], D. Goeckel, **S. Guha**[†], and D. Towsley, “Hiding Information in Noise: Fundamental Limits of Covert Communication,” IEEE Commun. Mag. **53** (12), 26-31 (Dec 2015).
 - [Bash15c] **B. A. Bash**[†], A.H. Gheorghe, M. Patel, **J. L. Habif**[†], D. Goeckel, D. Towsley, and **S. Guha**[†], “Quantum-secure Covert Communication on Bosonic Channels,” Nature Communications **6**, 8620 (2015).
 - [Sobers15] T. Sobers, **B. A. Bash**[†], D. Goeckel, **S. Guha**[†], and D. Towsley, “Covert Communication with the Help of an Uninformed Jammer Achieves Positive Rate,” Proc. Asilomar Conf. on Signals, Syst. and Comput., Pacific Grove, CA (2015)

References (3)

- Our work on covert communication (continued):
 - [Goeckel16] D. Goeckel, **B. A. Bash[†]**, **S. Guha[†]**, and D. Towsley, “Covert Communications when the Warden Does Not Know the Background Noise Power,” IEEE Communications Letters (2016)
 - [Sobers16] T. Sobers, **B. A. Bash[†]**, **S. Guha[†]**, D. Towsley, and D. Goeckel, “Covert Communication in the Presence of an Uninformed Jammer,” in submission (2016), arXiv:1608.00698v1 [cs.IT]
 - [Sheikholeslami16] A. Sheikholeslami, **B. A. Bash[†]**, D. Goeckel, D. Towsley, and **S. Guha[†]**, “Covert communication over classical-quantum channels,” Proc. IEEE Int. Symp. Inf. Theory (ISIT), Barcelona, Spain (2016) arXiv:1601.06826 [quant-ph]
 - [Soltani15] R. Soltani, D. Goeckel, D. Towsley, and A. Houmansadr, “Covert communications on poisson packet channels,” Proc. Conf. on Commun., Control, Comp. (Allerton), Monticello, IL (2015)
 - [Soltani16] R. Soltani, D. Goeckel, D. Towsley, and A. Houmansadr, “Covert communications on renewal packet channels,” arXiv:1610.00368 [cs.IT] (2016)

References (4)

- Sample of the follow-on work by other groups:
 - [Che13] P.H. Che, M. Bakshi, S. Jaggi “Reliable deniable communication: Hiding messages in noise,” Proc. IEEE Int. Symp. Inf. Theory (ISIT), Istanbul, Turkey (2013)
 - [Kadhe14] S. Kadhe, S. Jaggi, M. Bakshi, A. Sprintson, “Reliable, Deniable, and Hidable Communication over Multipath Networks,” Proc. IEEE Int. Symp. Inf. Theory (ISIT), Honolulu, Hawaii (2014).
 - [Hou14] J. Hou and G. Kramer, “Effective secrecy: Reliability, confusion and stealth,” Proc. IEEE Int. Symp. Inf. Theory (ISIT), Honolulu, Hawaii (2014)
 - [Che14] P.H. Che, M. Bakshi, C. Chan, S. Jaggi “Reliable Deniable Communication with Channel Uncertainty” Proc. IEEE Inf. Theory Workshop (ITW), Hobart, Australia (2014)
 - [Lee14] S. Lee, and R. J. Baxley, “Achieving positive rate with undetectable communication over AWGN and Rayleigh channels,” Proc. IEEE Int. Conf. Commun. (ICC) pp. 780-785, (2014).
 - [Lee15] S. Lee, R. J. Baxley, M.A. Weitnauer, and B. Walkenhorst, “Achieving Undetectable Communication,” IEEE J. Sel. Topics Signal Process., forthcoming.

References (5)

- Sample of the follow-on work by other groups (continued):
 - [Wang15] L. Wang, L. Zheng, G. W. Wornell, “Limits of Low-Probability-of-Detection Communication over a Discrete Memoryless Channel,” Proc. IEEE Int. Symp. Inf. Theory (ISIT), Hong Kong, China (2015).
 - [Bloch15] M. Bloch, “Covert Communication over Noisy Channels: A Resolvability Perspective,” Proc. IEEE Int. Symp. Inf. Theory (ISIT), Hong Kong, China (2015), arXiv:1503.08778 [cs.IT] (2015)
 - [Tahmasbi16] M. Tahmasbi and M. Bloch, “Second-Order Asymptotics of Covert Communications over Noisy Channels,” Proc. IEEE Int. Symp. Inf. Theory (ISIT), Barcelona, Spain (2016)
 - [Arumugam16a] K.S.K. Arumugam and M. Bloch “Keyless Covert Communication over Multiple-Access Channels,” Proc. IEEE Int. Symp. Inf. Theory (ISIT), Barcelona, Spain (2016)
 - [Zhang16] Q. Zhang, M. Bakshi, and S. Jaggi, “Computationally Efficient Deniable Communication,” Proc. IEEE Int. Symp. Inf. Theory (ISIT), Barcelona, Spain (2016)
 - [Arumugam16b] K.S.K. Arumugam and M. Bloch “Keyless asynchronous covert communication,” Proc. Inform. Theory Workshop (ITW), Cambridge, UK (2016)