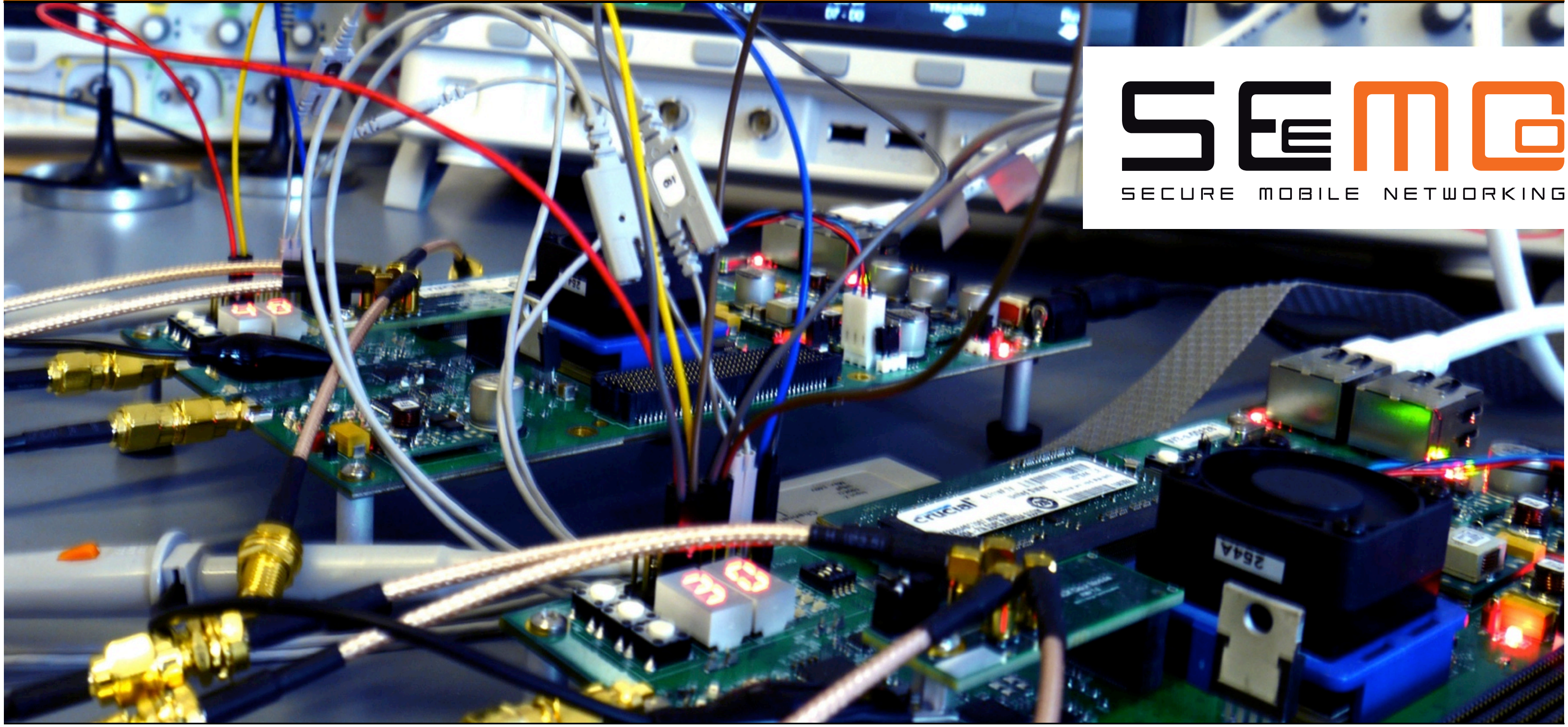
Practical Known-Plaintext Attacks against Physical Layer Security in Wireless MIMO Systems

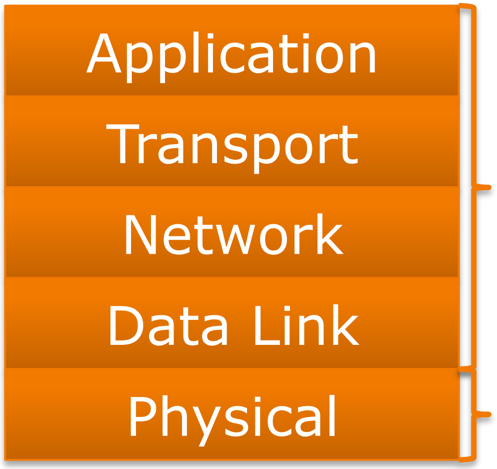
Matthias Schulz, Adrian Loch, Matthias Hollick

TECHNISCHE UNIVERSITÄT DARMSTADT



SEEMOO SECURE MOBILE NETWORKING

Motivation



Cryptography

computational security

powerful attack models

Physical Layer Security

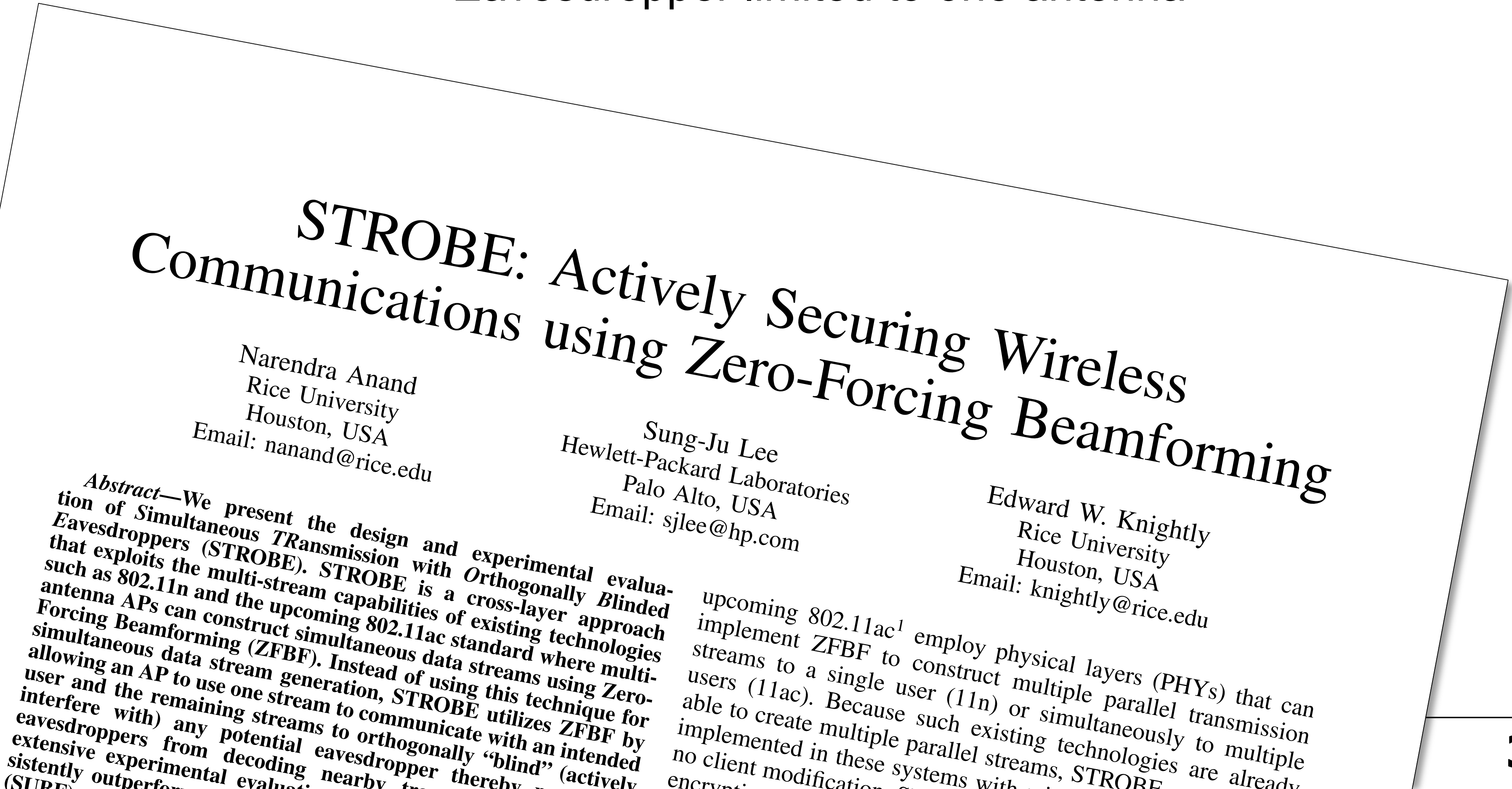
aims at information-theoretical security

no computational restrictions on eavesdropper

Motivation

STROBE: Orthogonal Blinding

- Published at INFOCOM 2012
- Practical Orthogonal Blinding implementation
- Eavesdropper limited to one antenna



STROBE: Actively Securing Wireless Communications using Zero-Forcing Beamforming

Narendra Anand
Rice University
Houston, USA
Email: nanand@rice.edu

Sung-Ju Lee
Hewlett-Packard Laboratories
Palo Alto, USA
Email: sjlee@hp.com

Edward W. Knightly
Rice University
Houston, USA
Email: knightly@rice.edu

***Abstract*—We present the design and experimental evaluation of *S*imultaneous *TR*ansmission with *O*rthogonally *B*linded *E*avesdroppers (STROBE). STROBE is a cross-layer approach that exploits the multi-stream capabilities of existing technologies such as 802.11n and the upcoming 802.11ac standard where multi-antenna APs can construct simultaneous data streams using Zero-Forcing Beamforming (ZFBF). Instead of using this technique for simultaneous data stream generation, STROBE utilizes ZFBF by allowing an AP to use one stream to communicate with an intended user and the remaining streams to orthogonally "blind" (actively interfere with) any potential eavesdropper thereby p eavesdroppers from decoding nearby tra extensive experimental evaluati sistently outperfor (SURF)**

upcoming 802.11ac[1] employ physical layers (PHYs) that can implement ZFBF to construct multiple parallel transmission streams to a single user (11n) or simultaneously to multiple users (11ac). Because such existing technologies are already able to create multiple parallel streams, STROBE implemented in these systems with no client modification encrypti

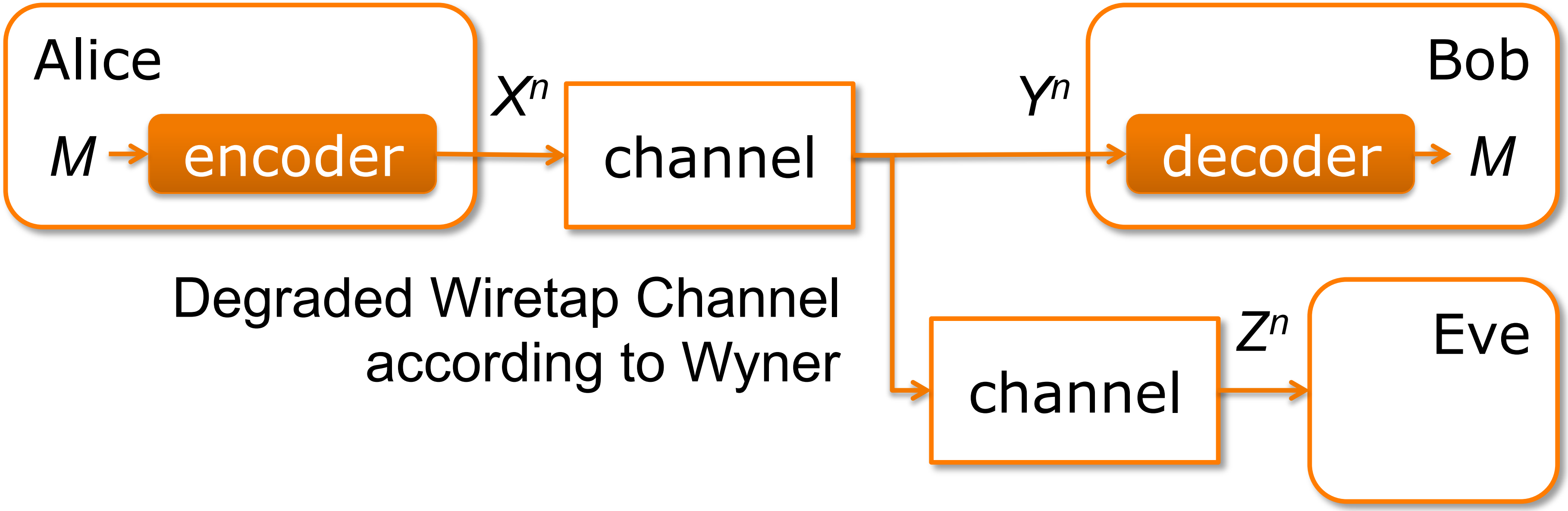
Contents

- Motivation
- Introduction to Orthogonal Blinding
- Contribution: Known-Plaintext Attack
- Evaluation
- Conclusion

Contents

- Motivation
- **Introduction to Orthogonal Blinding**
- Contribution: Known-Plaintext Attack
- Evaluation
- Conclusion

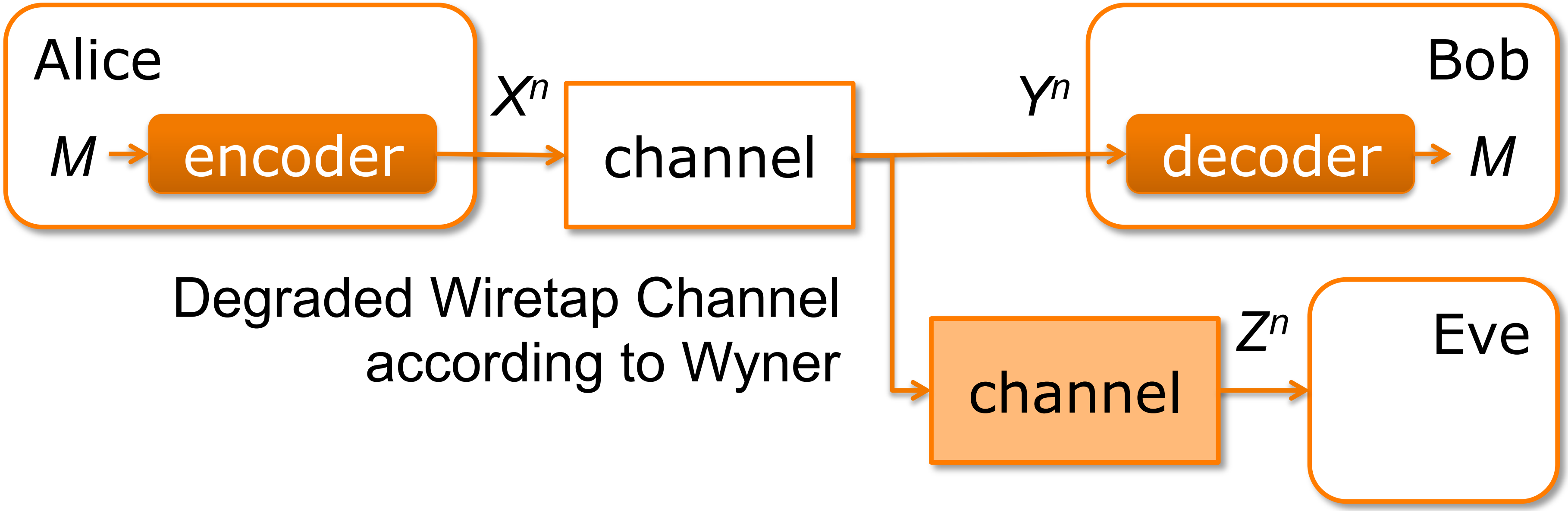
From Shannon to Wyner



Degraded Wiretap Channel according to Wyner

→ Secrecy measured as information leakage to Eve

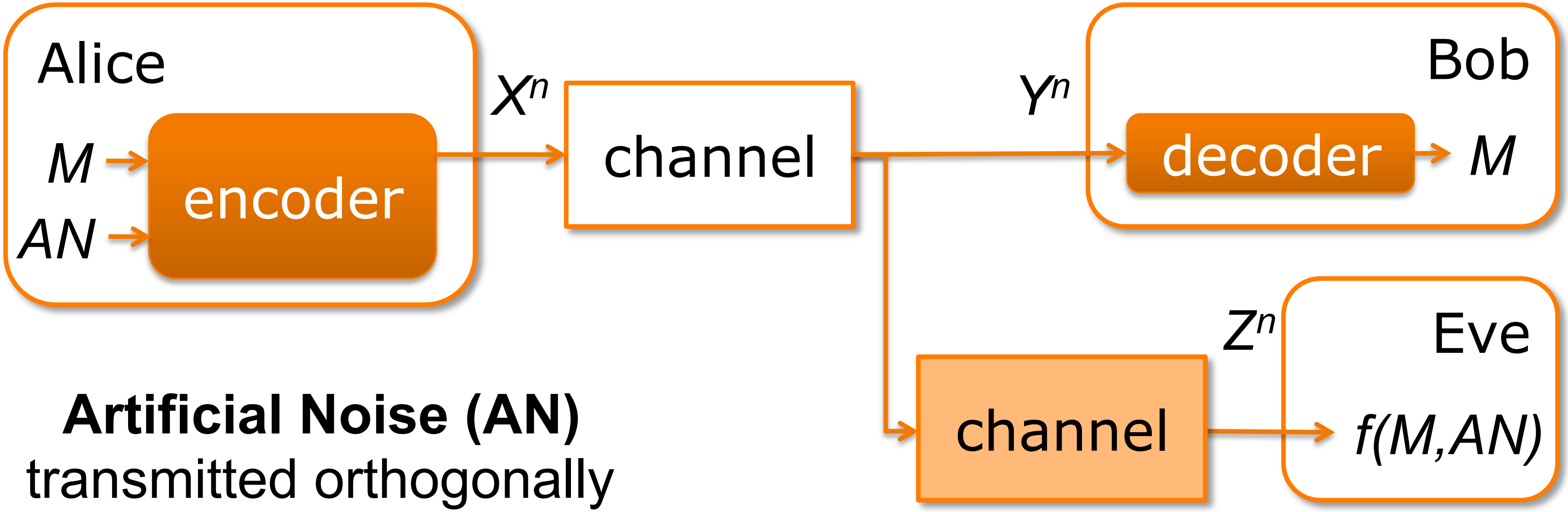
How to reduce information leakage?



Degraded Wiretap Channel according to Wyner

The channel to Eve should introduce additional noise

Orthogonal Blinding

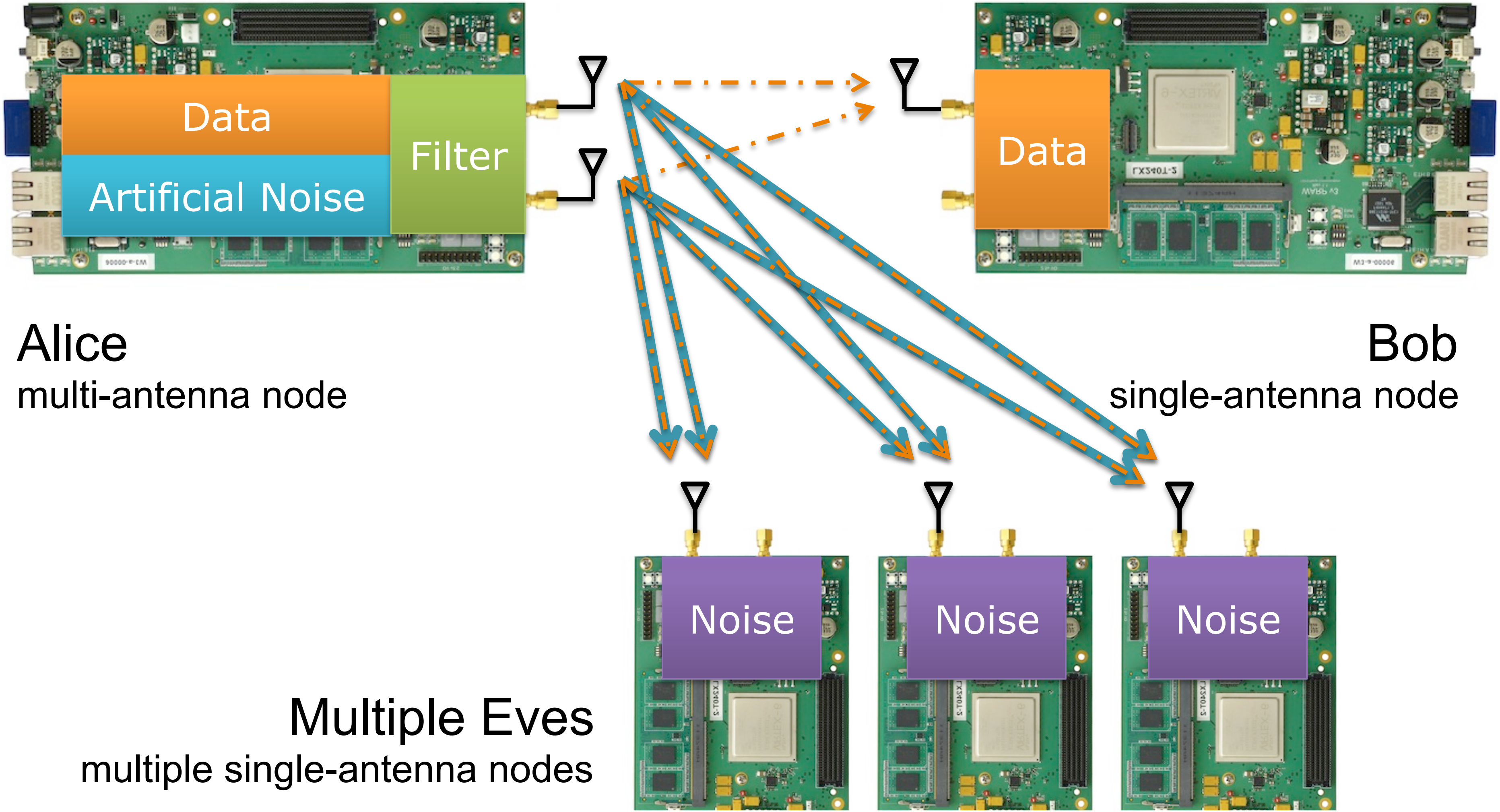


Artificial Noise (AN)
transmitted orthogonally
to Bob's channel:
"blinding" only Eve

The channel to Eve should
introduce additional noise

Orthogonal Blinding

Practical Implementation



Alice
multi-antenna node

Bob
single-antenna node

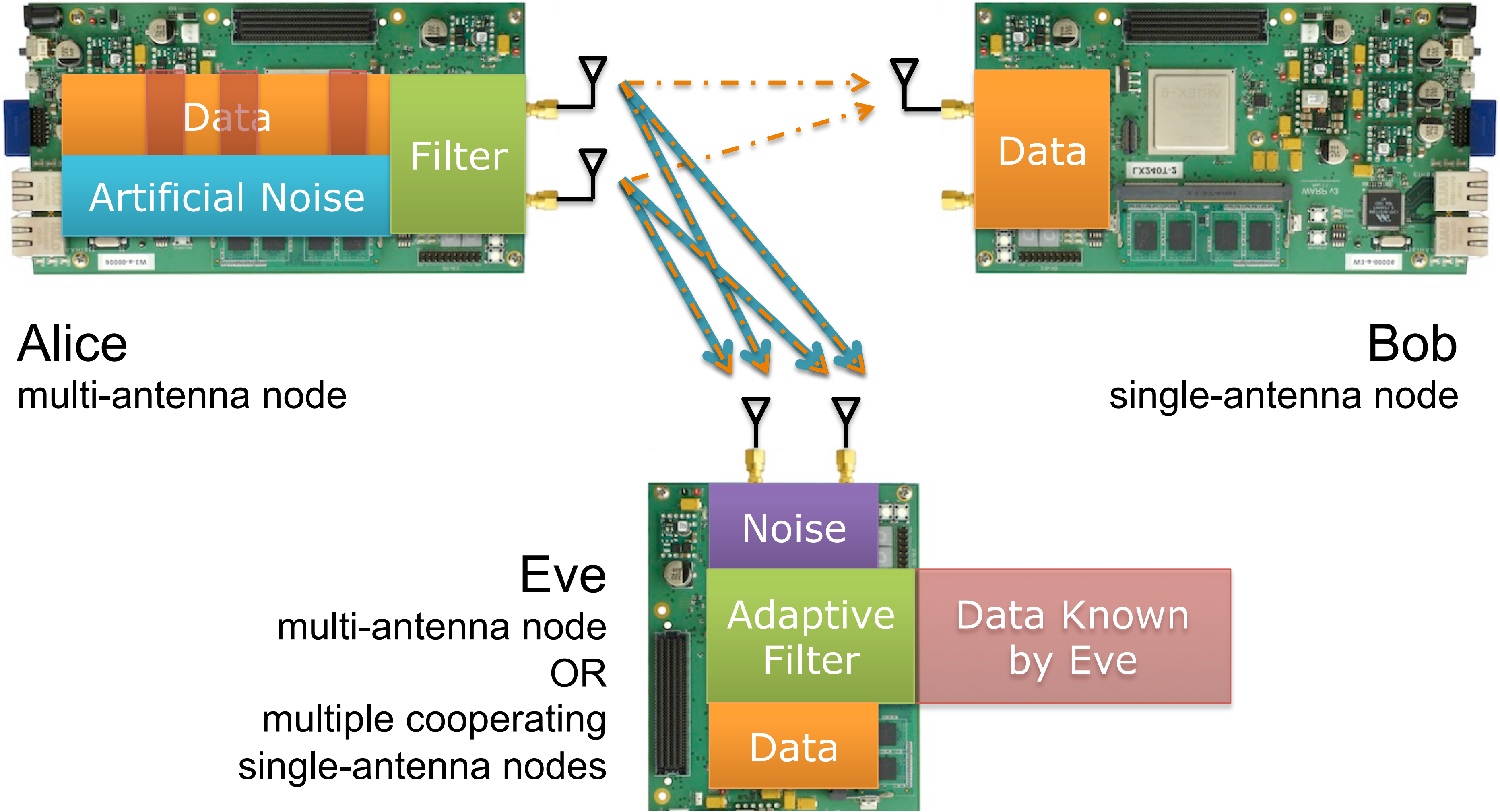
Multiple Eves
multiple single-antenna nodes

Contents

- Motivation
- Introduction to Orthogonal Blinding
- Contribution: Known-Plaintext Attack
- Evaluation
- Conclusion

Known Plaintext Attack

System Model



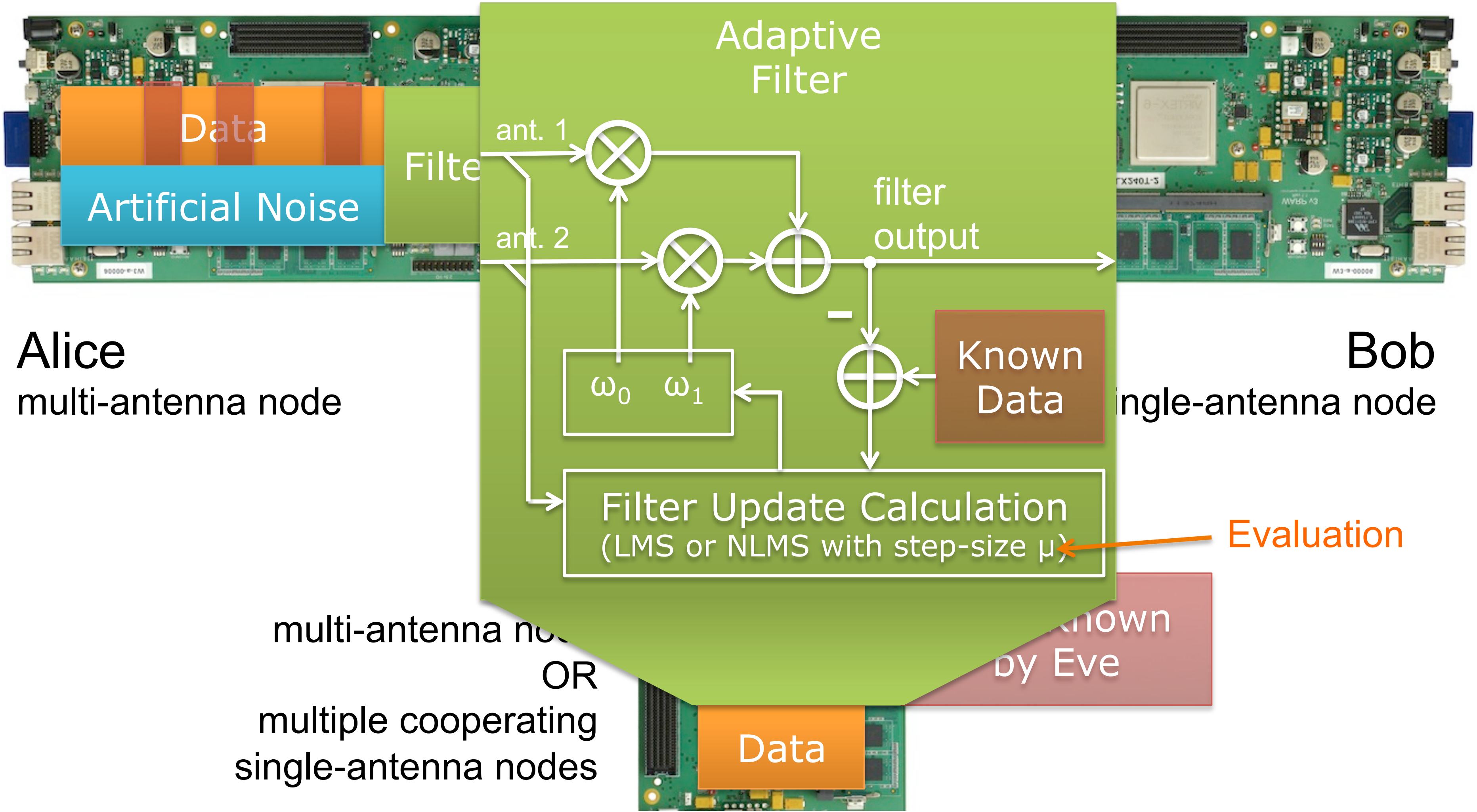
Alice
multi-antenna node

Bob
single-antenna node

Eve
multi-antenna node
OR
multiple cooperating
single-antenna nodes

Known Plaintext Attack

System Model



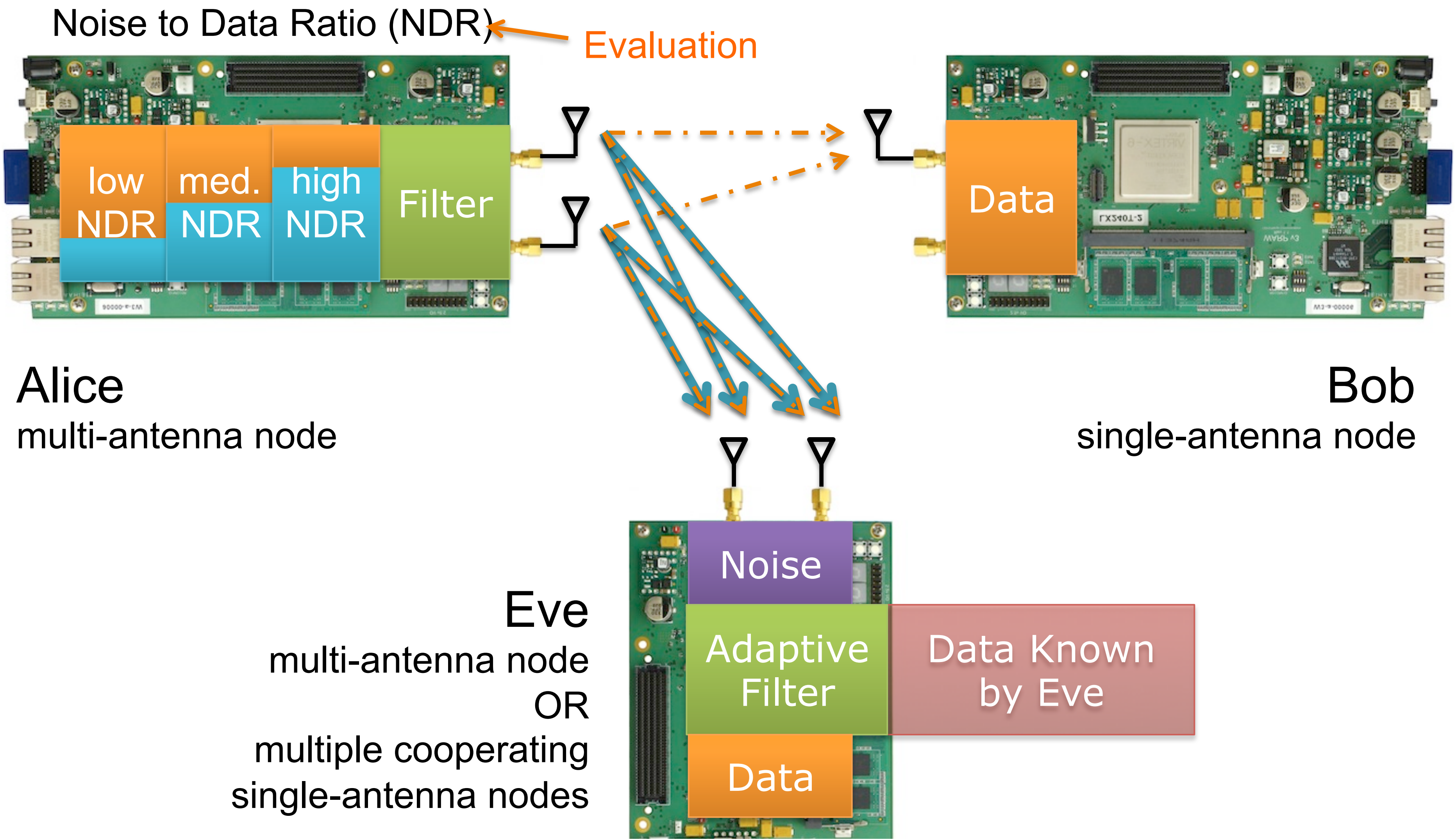
Alice
multi-antenna node

Bob
single-antenna node

multi-antenna node
OR
multiple cooperating
single-antenna nodes

Known Plaintext Attack

Noise to Data Ratio



Noise to Data Ratio (NDR)

Evaluation

low NDR

med. NDR

high NDR

Filter

Data

Alice

multi-antenna node

Bob

single-antenna node

Eve

multi-antenna node

OR

multiple cooperating single-antenna nodes

Noise

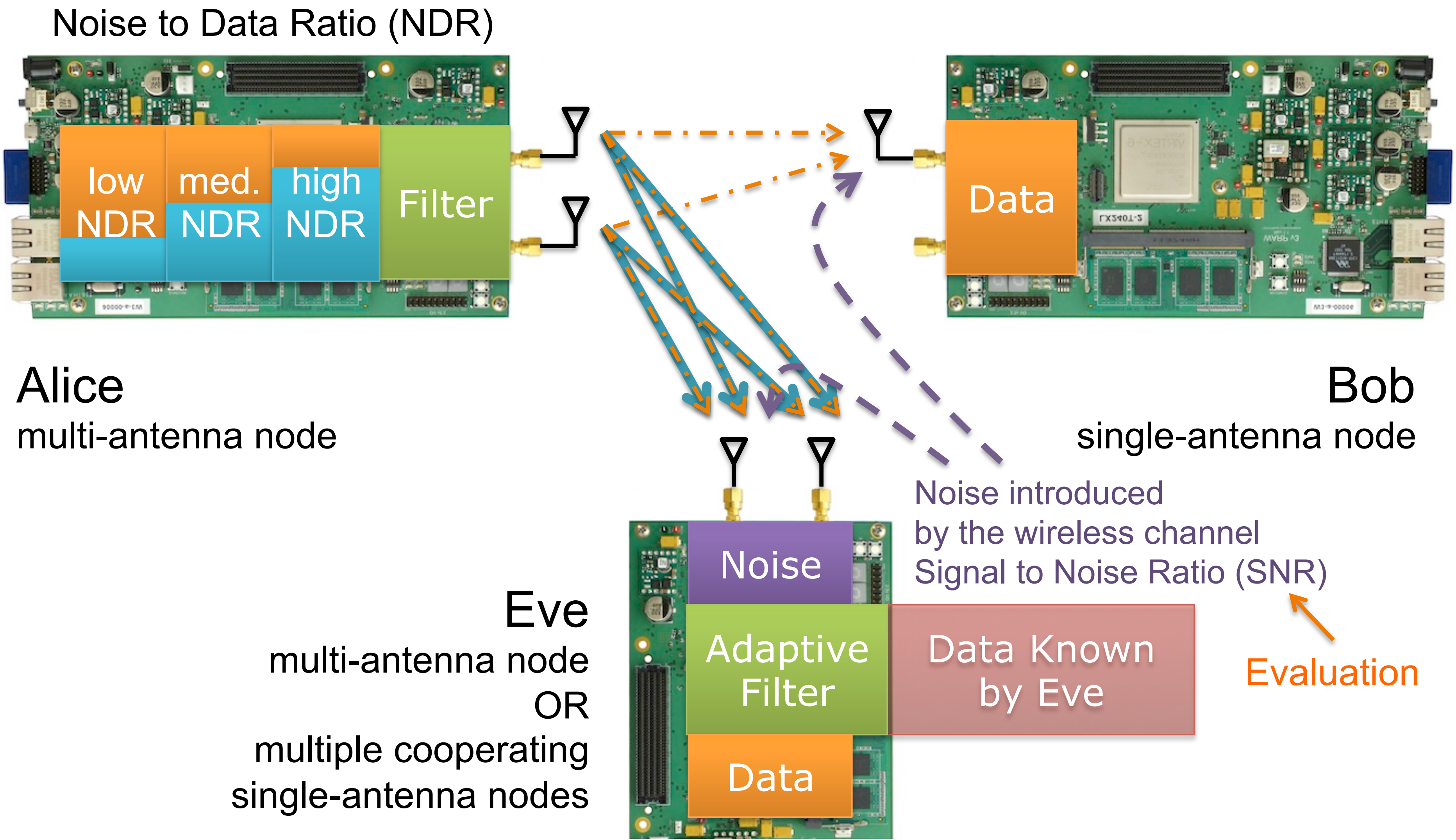
Adaptive Filter

Data Known by Eve

Data

Known Plaintext Attack

Noise introduced by Wireless Channel

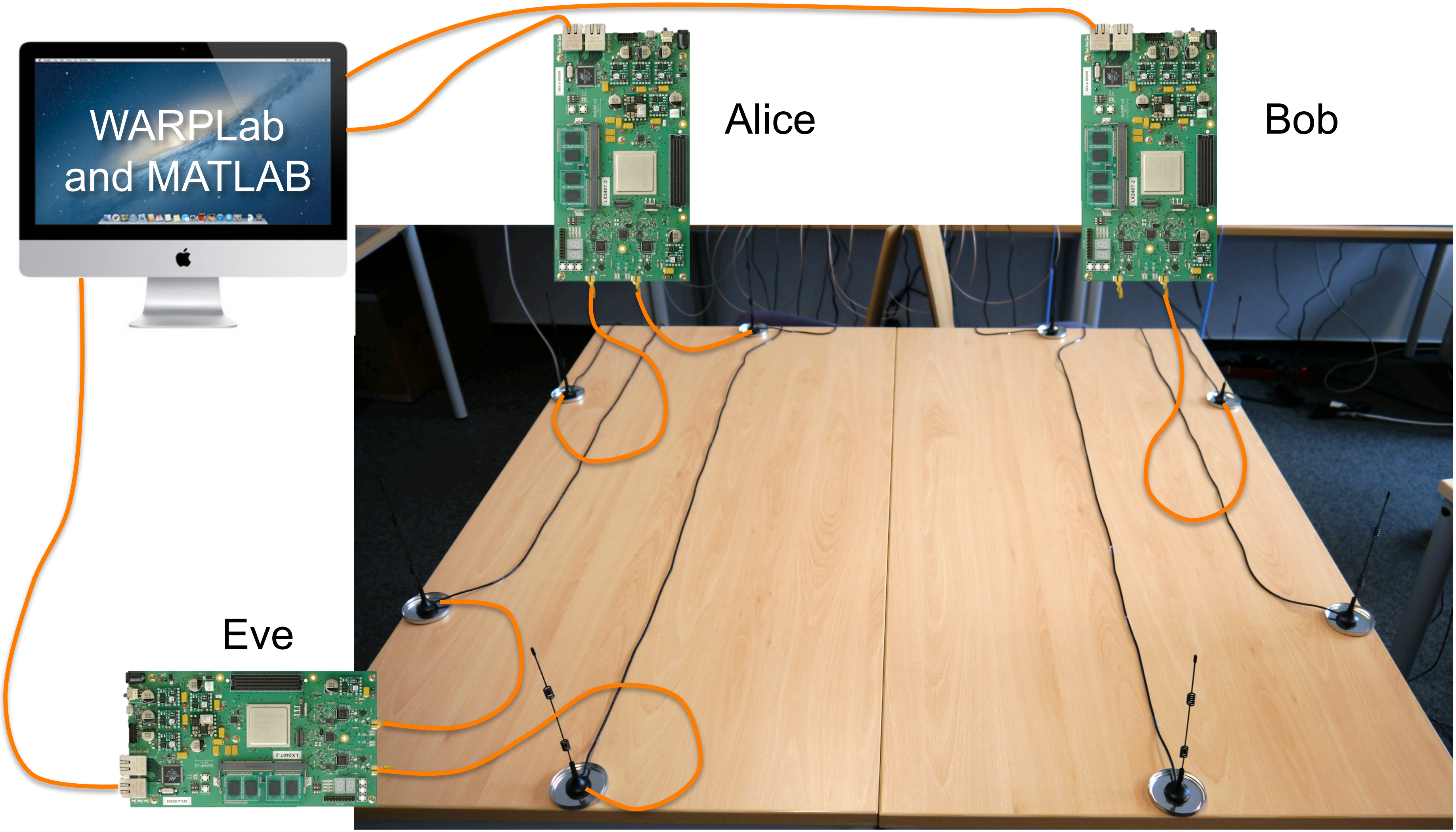


Contents

- Motivation
- Introduction to Orthogonal Blinding
- Contribution: Known-Plaintext Attack
- Evaluation
- Conclusion

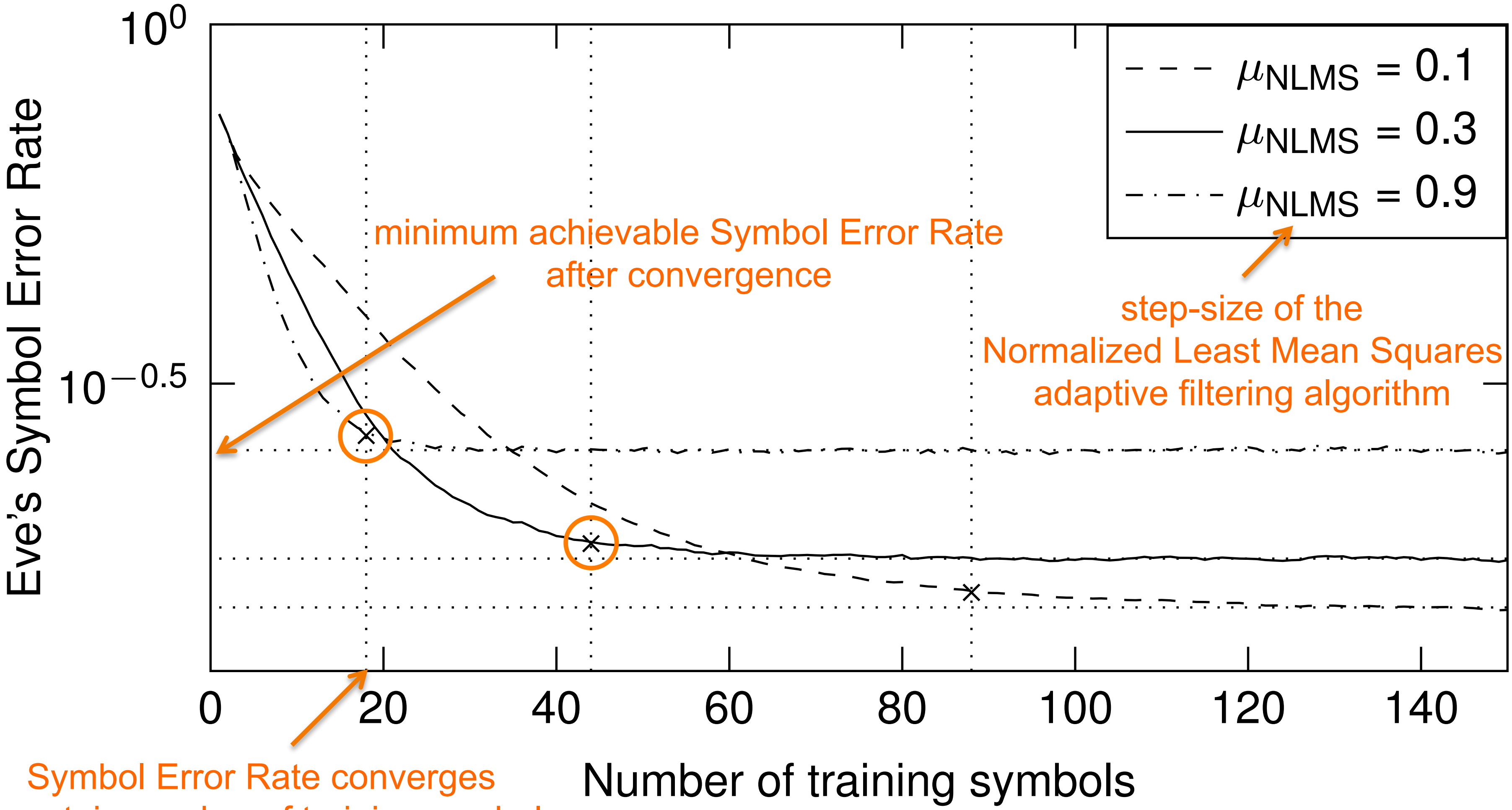
Evaluation

Testbed



Evaluation

Eve’s Filter Convergence (measurement)



minimum achievable Symbol Error Rate after convergence

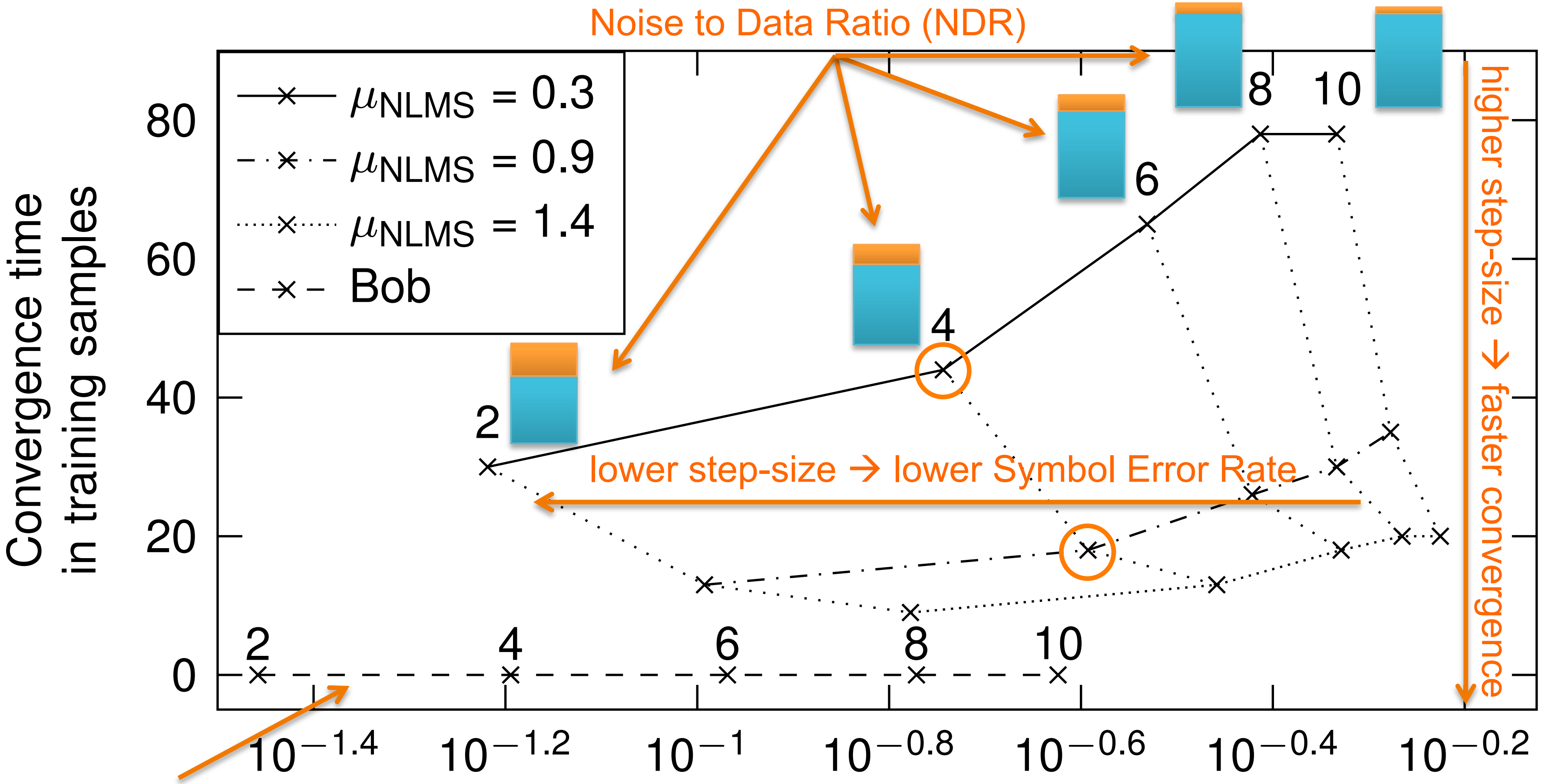
step-size of the Normalized Least Mean Squares adaptive filtering algorithm

Symbol Error Rate converges for certain number of training symbols

Noise to Data Ratio (NDR) = 4

Evaluation

Convergence performance (measurement)

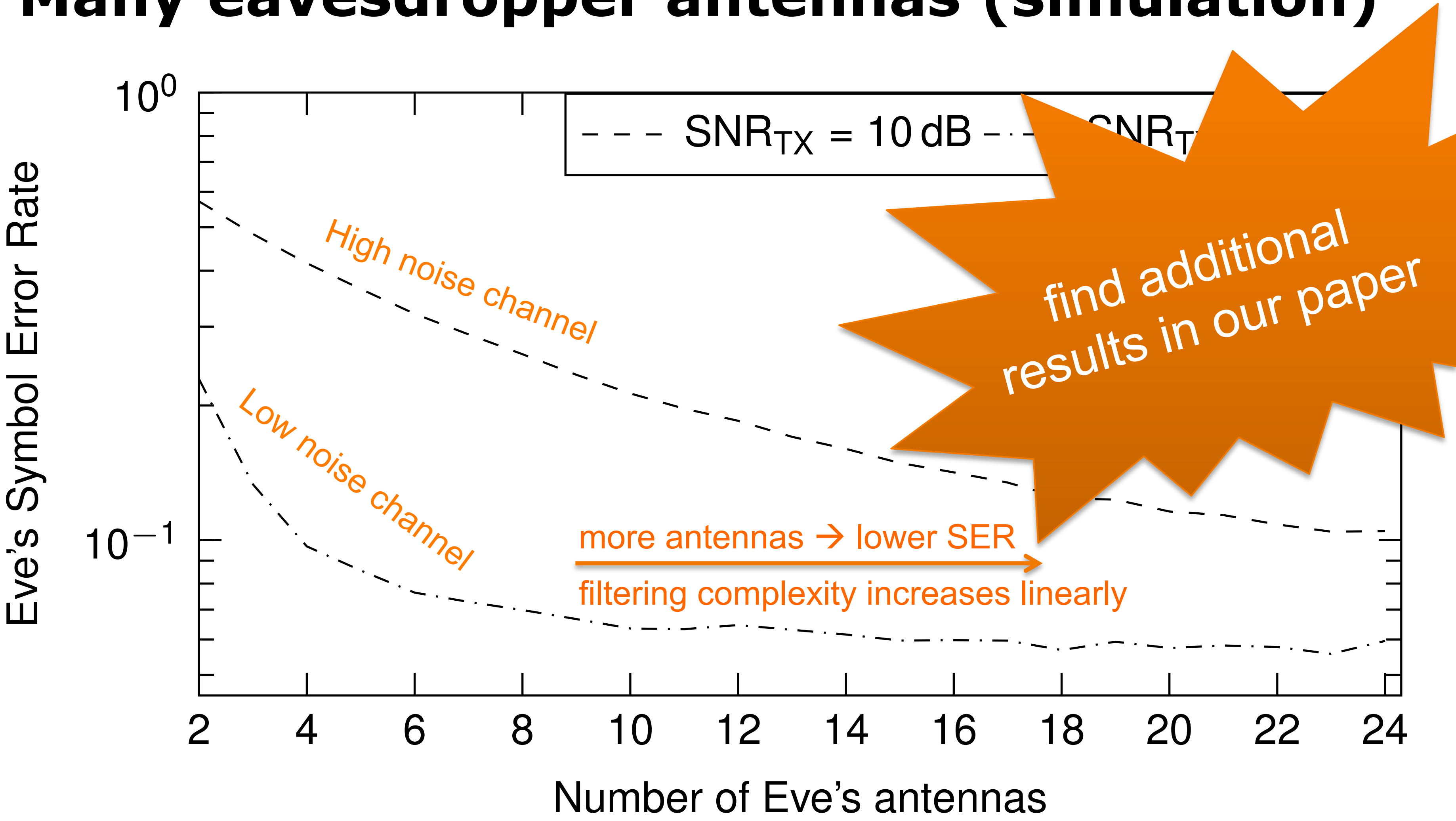


Eve's Symbol Error Rate at convergence

For comparison:
Bob's Symbol Error Rate

Evaluation

Many eavesdropper antennas (simulation)



find additional results in our paper

more antennas → lower SER

filtering complexity increases linearly

100 training symbols, Noise to Data Ratio (NDR) = 10, filter step-size: $\mu_{\mathrm{NLMS}} = 0.3$

Contents

- Motivation
- Introduction to Orthogonal Blinding
- Contribution: Known-Plaintext Attack
- Evaluation
- Conclusion

Conclusion

- Successful secrecy reduction
- Adaptive filtering used for known-plaintext attacks
- Simulation and experimental evaluation

If you ever propose a physical layer security scheme
→ → → consider multi-antenna eavesdroppers ← ← ←

Thank you for your attention

SEEMOO
SECURE MOBILE NETWORKING

TECHNISCHE UNIVERSITÄT DARMSTADT

Matthias Schulz
Department of Computer Science

SEEMOO
Mornewegstr. 32
64293 Darmstadt/Germany
mschulz@seemoo.tu-darmstadt.de

Phone +49 6151 16-70928
Fax +49 6151 16-70921
www.seemoo.tu-darmstadt.de