PhyAuth: Physical-Layer Message Authentication for ZigBee Networks

Ang Li[1,2], Jiawei Li[1], Dianqi Han[3]

Yan Zhang[4], Tao Li[5], Ting Zhu[6], Yanchao Zhang[1]

[1]Arizona State University

[2]University of Michigan-Dearborn

[3]University of Texas at Arlington

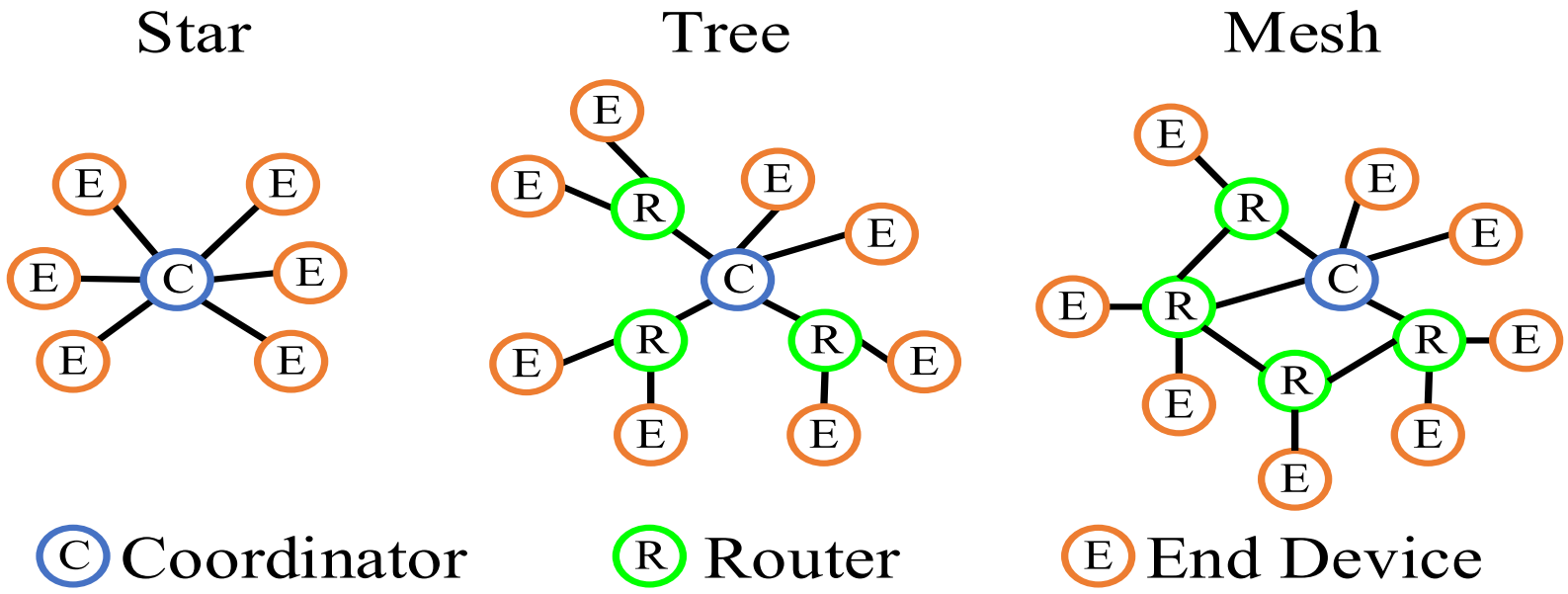
[4]The University of Akron

[5]Indiana University-Purdue University Indianapolis

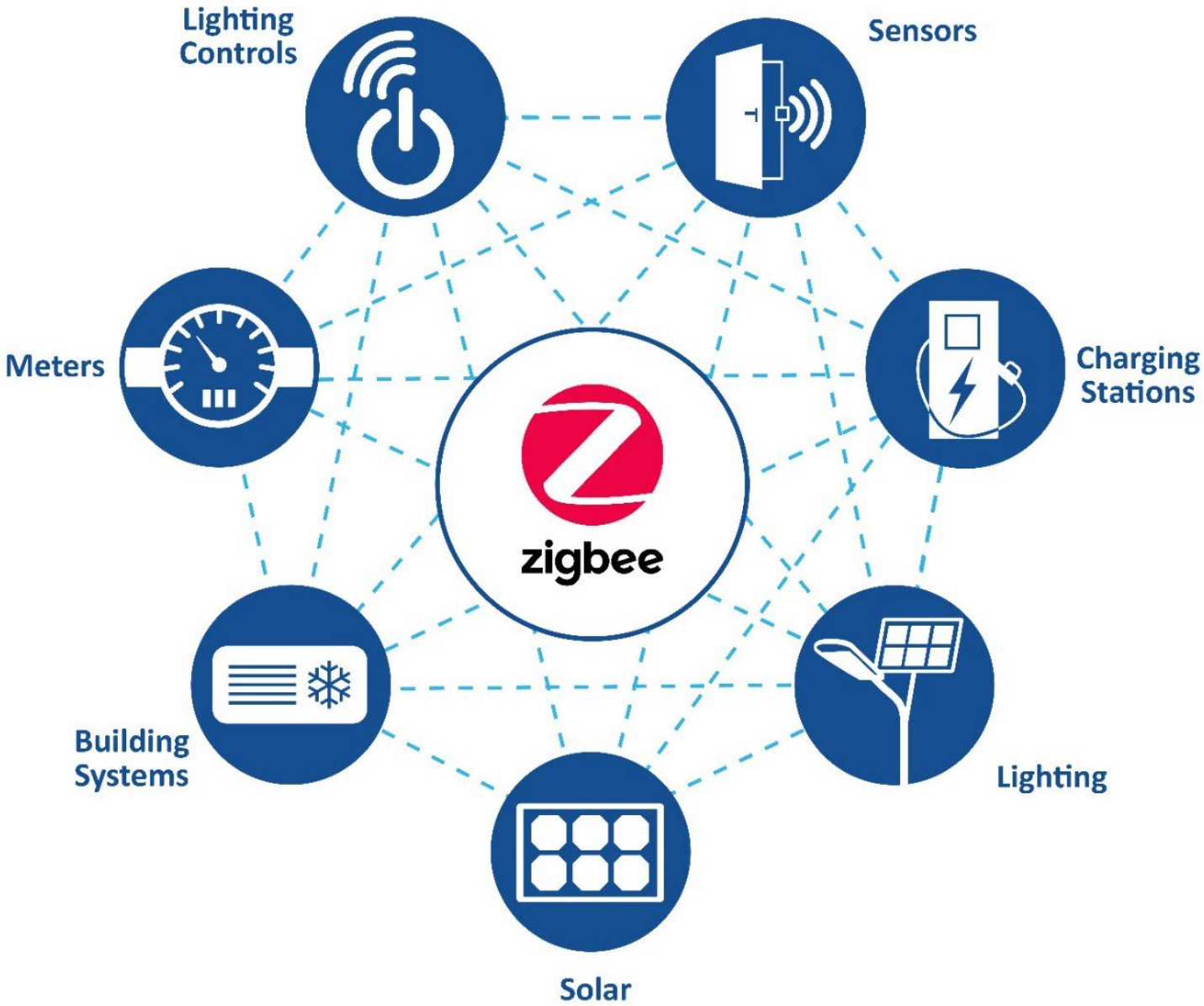
[6]The Ohio State University

What is ZigBee?

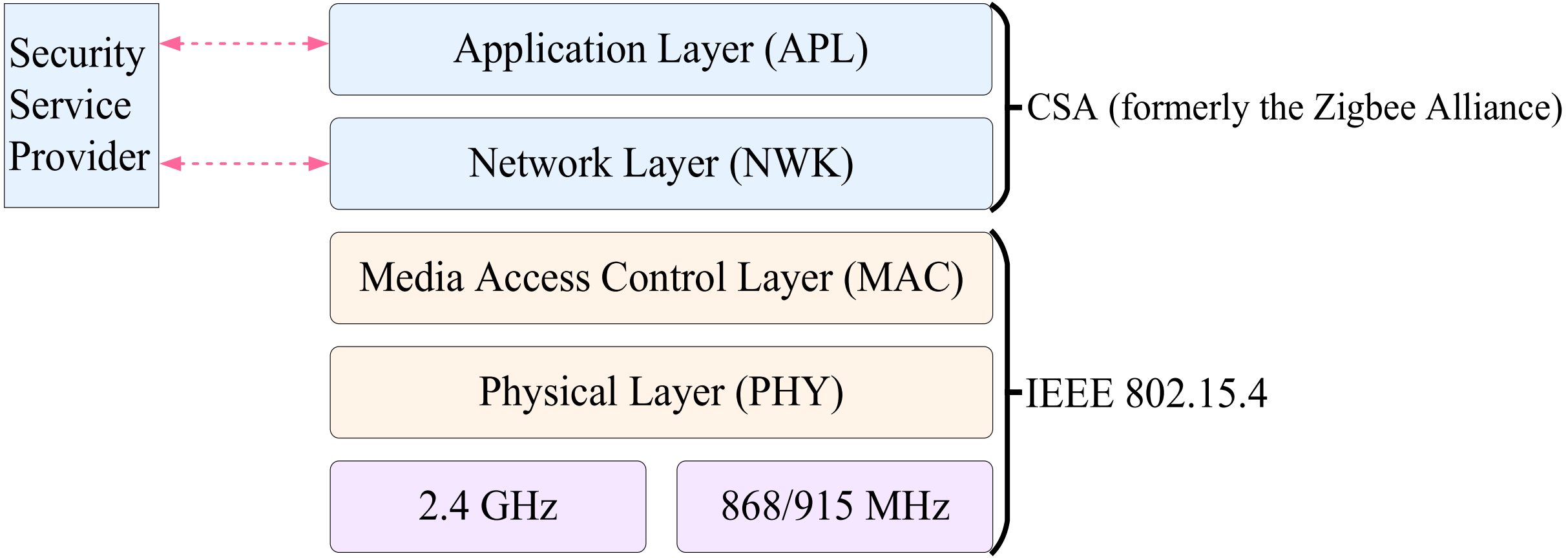
- IEEE 802.15.4-based
- Low-power, low-data-rate
- 2.4 GHz, 900 MHz, and 868 MHz frequency bands



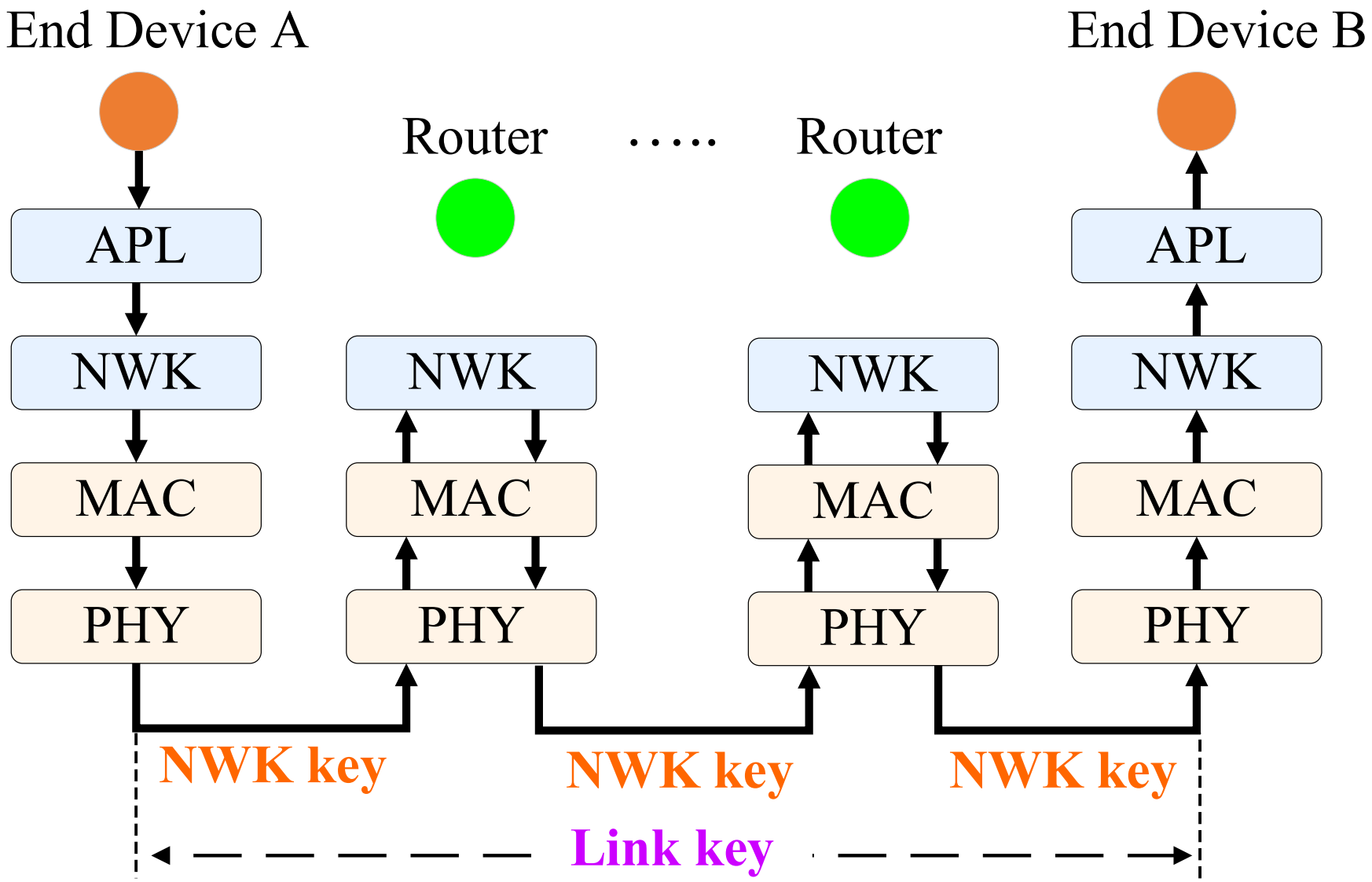
ZigBee Applications



ZigBee Architecture & Security Mechanism



ZigBee Security Mechanism



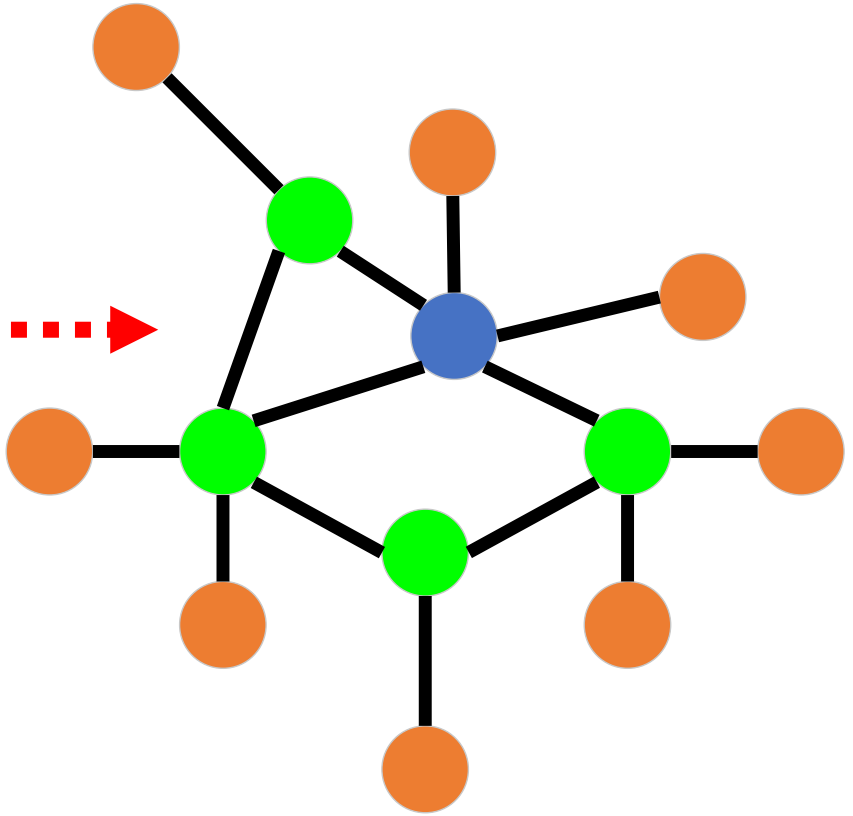
Vulnerability in ZigBee networks

NWK key is a group key

↓

NWK key could be compromised by adversaries

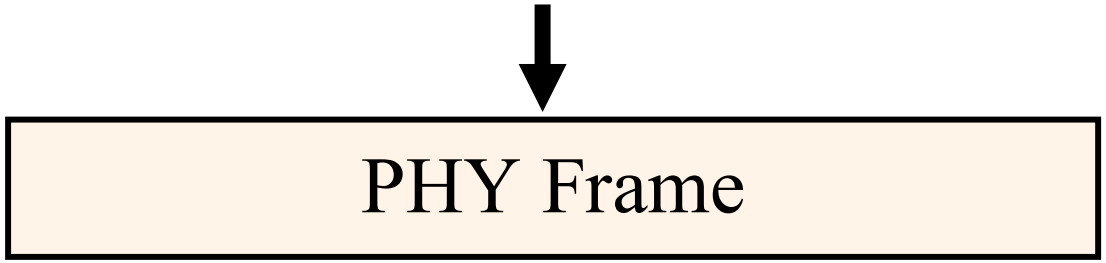
Fake packets



PhyAuth

- PHY hop-by-hop message authentication framework
- Motivation
  - Protocol compatibility
  - The implementation of PHY is determined by vendors
- Key idea

PHY one-time password (**POPT**)



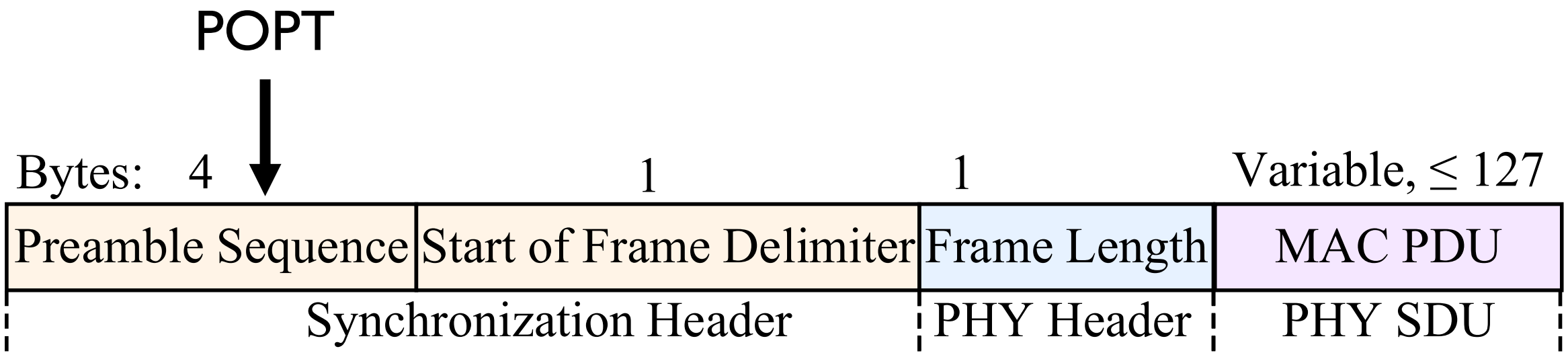
POTP Generation

$$\text{POTP}(K, T, SN, src\text{-}addr) = \text{Truncate}\left(HMAC^{1}(K, T, SN, src\text{-}addr)\right)$$

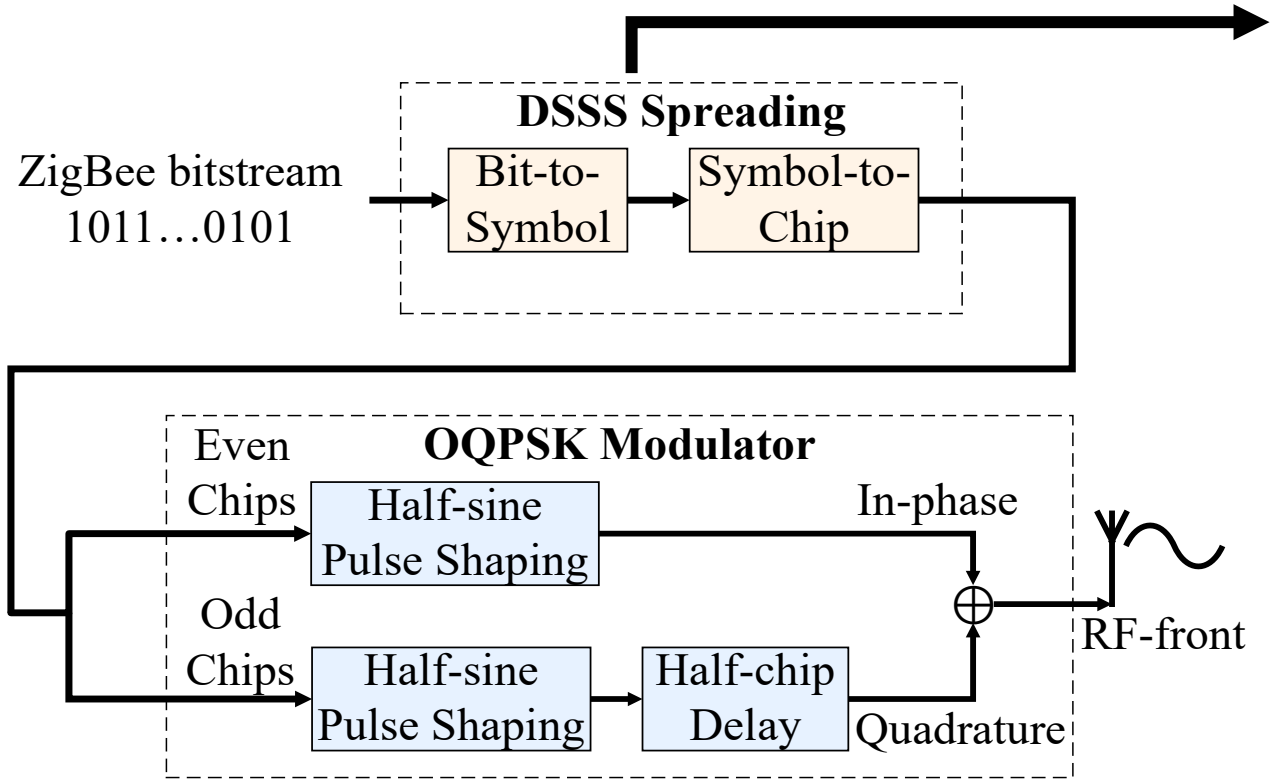
- **K**: a standard ZigBee security key (e.g., link key)
- **T:** $\frac{T_C - T_0}{X}$, T_C is the current timestamp, T_0 is the start timestamp.
- **SN:** 8-bit monotonically increasing sequence number in the 802.15.4 MAC frame header
- **src-addr:** the transmitter's 64-bit MAC address

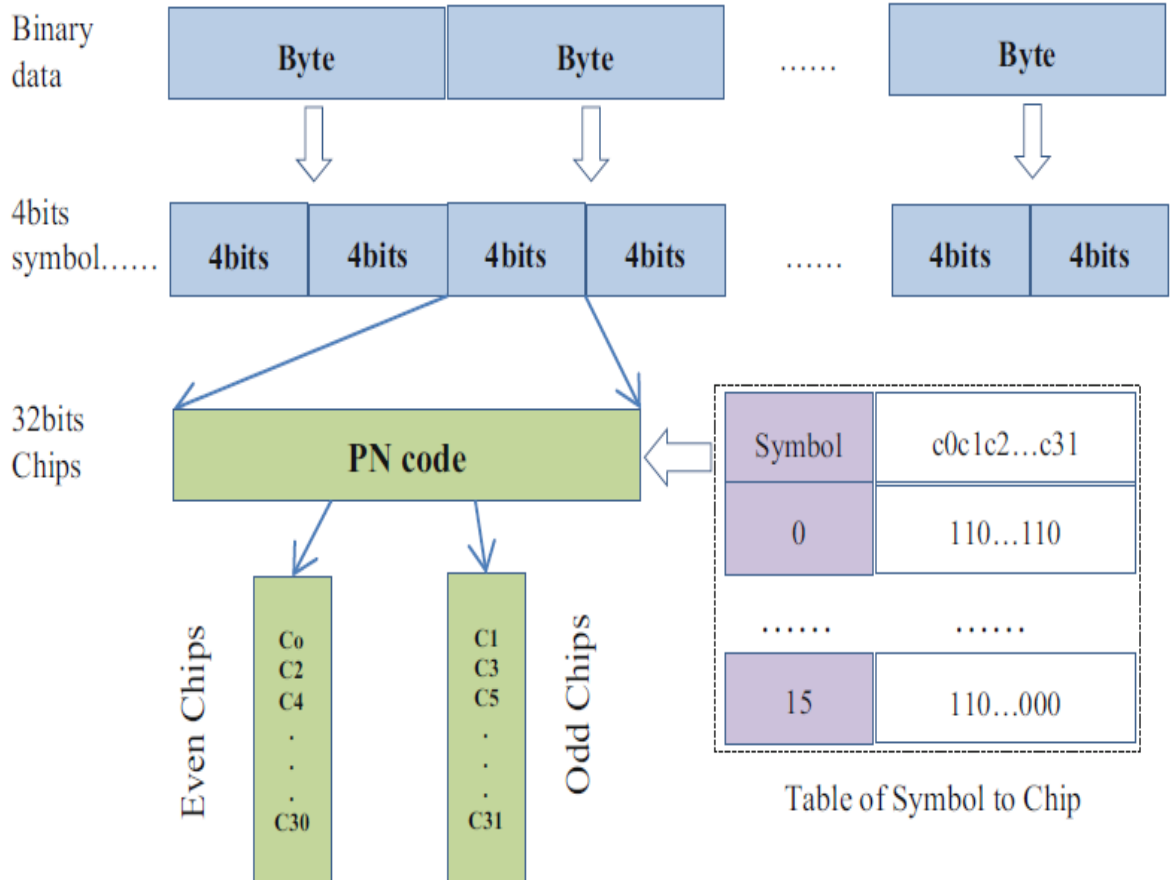
1. RFC 4226 and RFC 6238

ZigBee PHY Frame



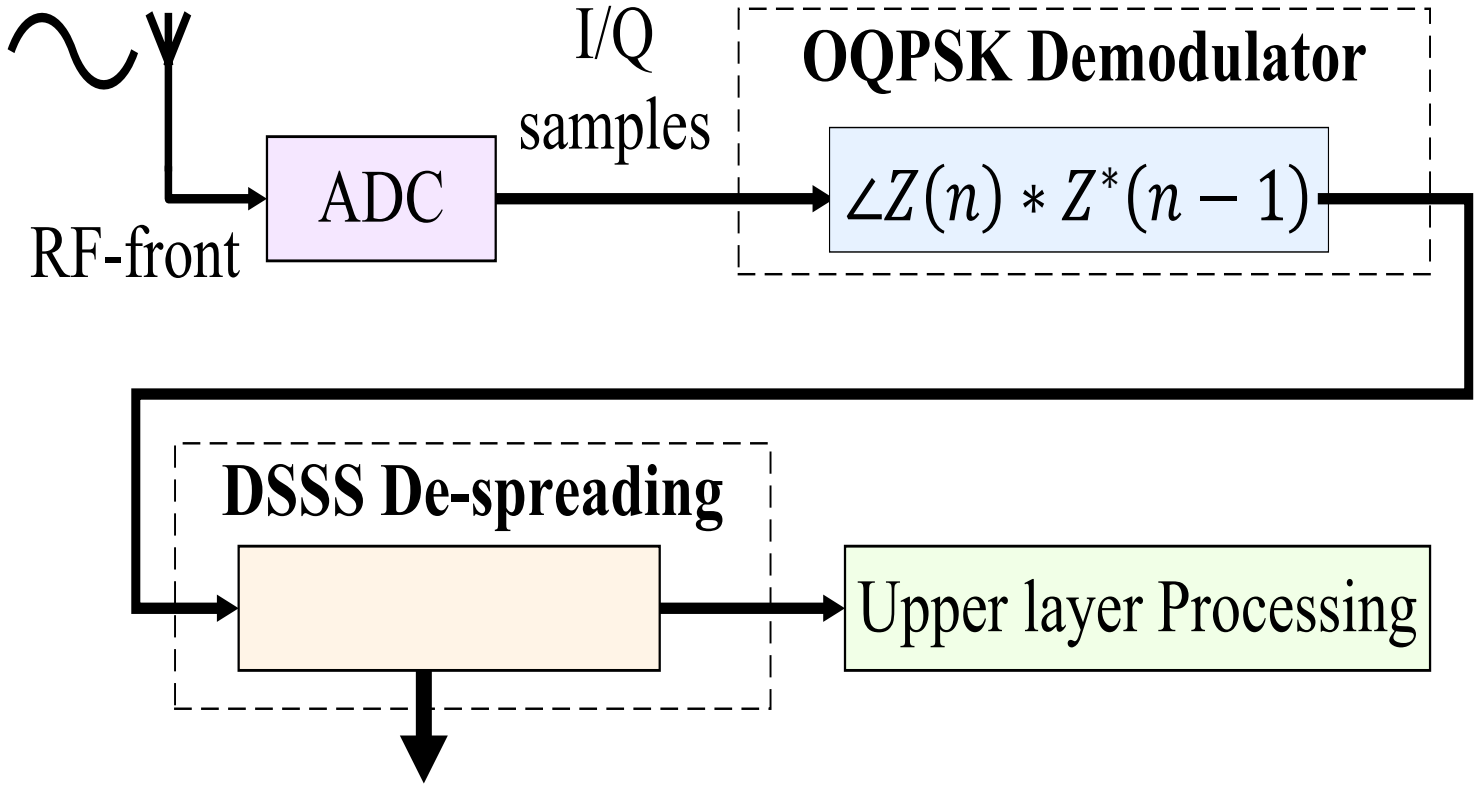
VarChip—Observation





Transmitter

VarChip—Observation



Symbol = $\min_{\{i|0x0 \le i \le 0xF\}} \{d^H(PN_r, PN_i) | d^H(PN_r, PN_i) \le \theta\}$

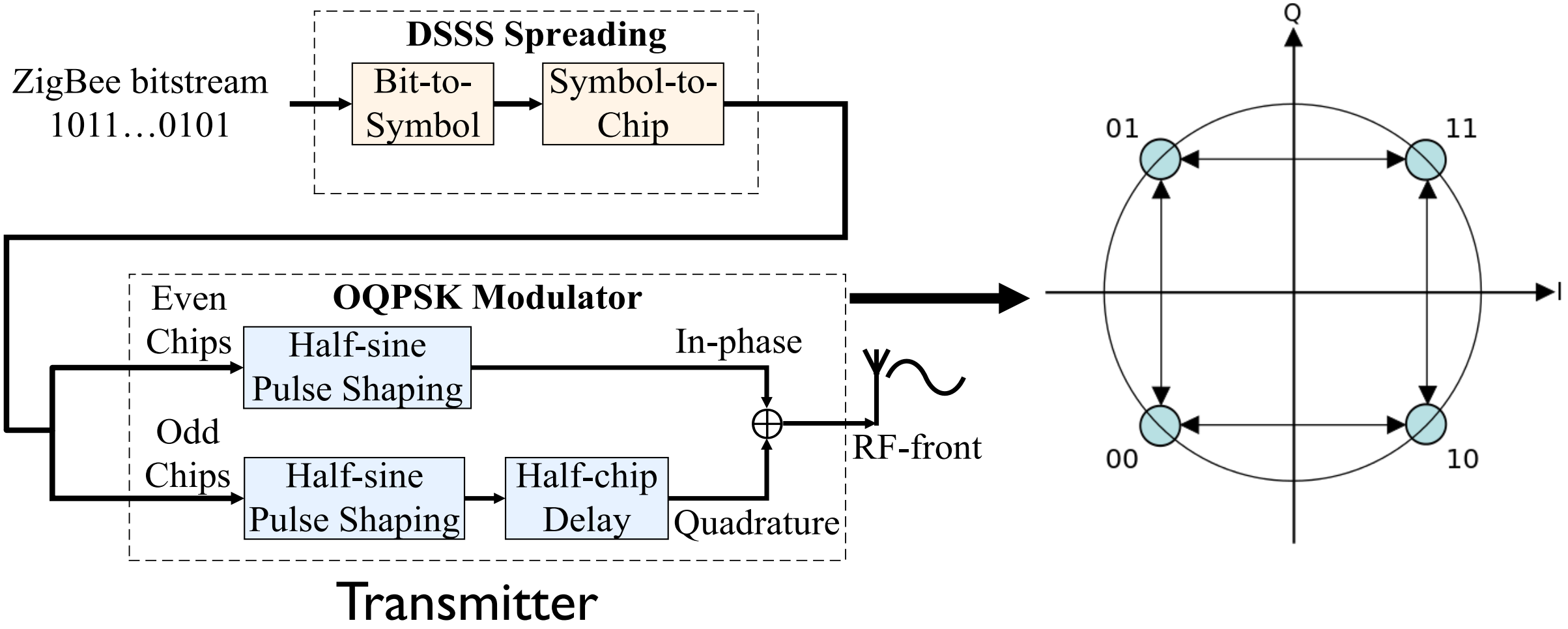
d^H is Hamming distance

VarChip—Key Idea

$$\text{Symbol} = \min_{\{i|0x0 \le i \le 0xF\}} \{d^H(PN_r, PN_i) | d^H(PN_r, PN_i) \le \theta\}$$

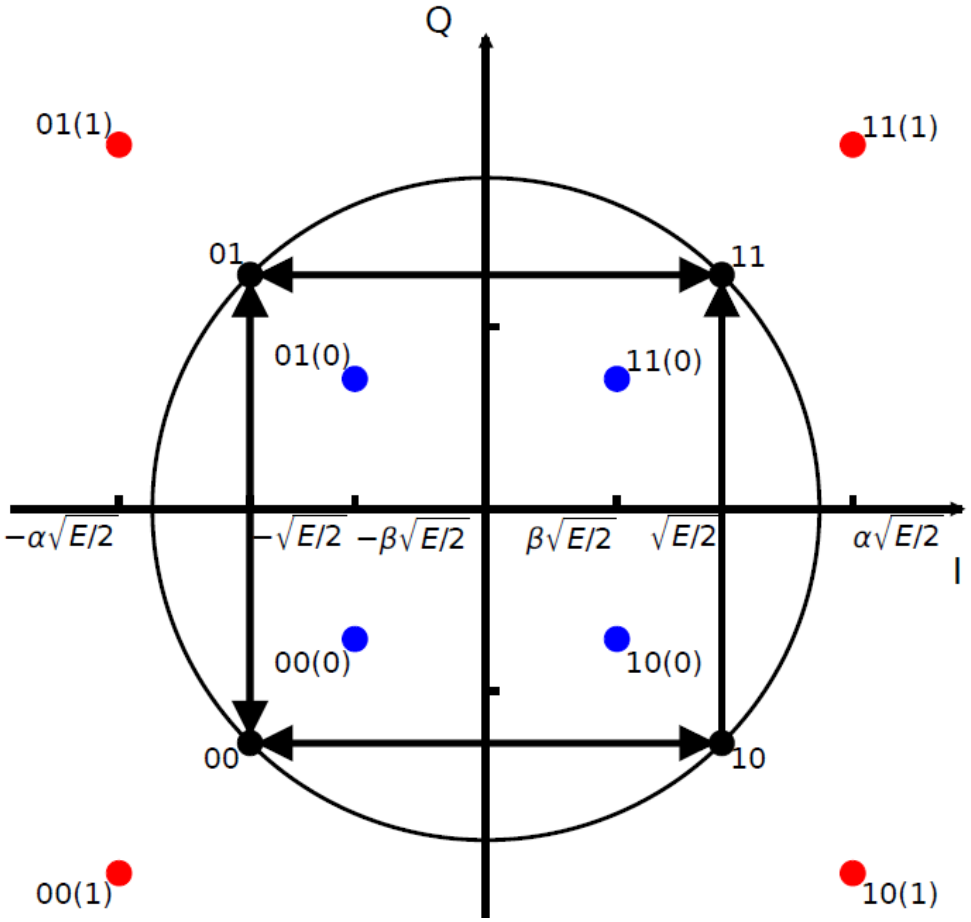
Substitute POTP bits for chips with a low error probability

VarAmp—Observation



Amplitudes of OQPSK symbols do not carry any information bits

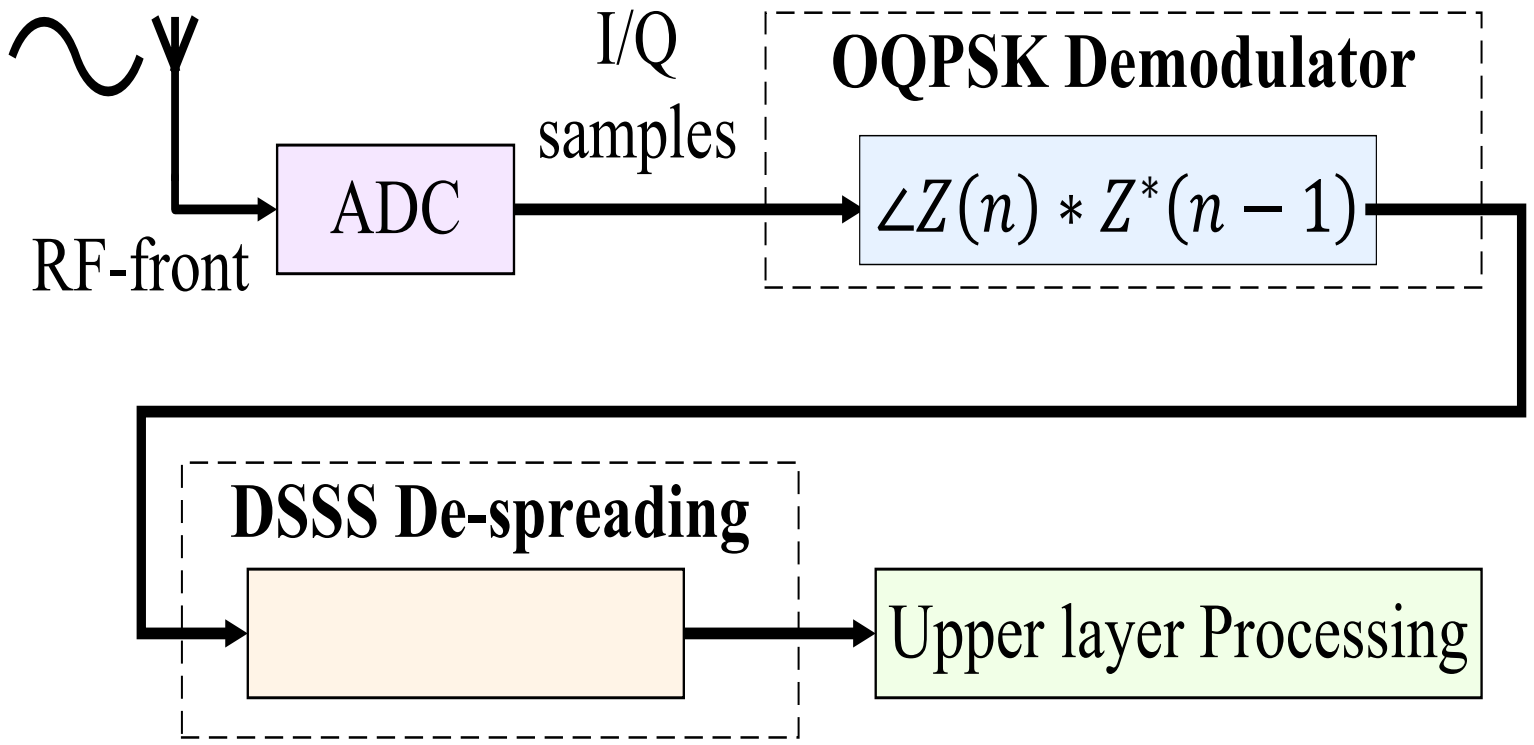
VarAmp—Key idea



$$\text{Manipulated amplitude} = \begin{cases} \alpha A_0 & POTP\ bit\ is\ 1, \alpha \geq 1 \\ \beta A_0 & POTP\ bit\ is\ 0, 0 \leq \beta < 1 \end{cases}$$

VarPhase—Observation

Receiver



$$\text{Received data bit} = \begin{cases} 1 & \tan^{-1}\left(Z(n) * Z^*(n-1)\right) \geq 0 \\ 0 & \tan^{-1}\left(Z(n) * Z^*(n-1)\right) < 0 \end{cases}$$

VarPhase—Key idea

$$\text{Received data bit} = \begin{cases} 1 & \tan^{-1}\left(Z(n) * Z^*(n-1)\right) \geq 0 \\ 0 & \tan^{-1}\left(Z(n) * Z^*(n-1)\right) < 0 \end{cases}$$

Embed a POTP into PHY packets by manipulating the phase shift between consecutive I/Q data samples

VarPhase—Key idea

Embed a POTP into PHY packets by manipulating the phase shift between consecutive I/Q data samples

$$\text{Manipulated phase shift} = \begin{cases} \lambda\Delta\phi_0 & POTP\ bit\ is\ 1, \lambda > \mu \\ \mu\Delta\phi_0 & POTP\ bit\ is\ 0, \mu \geq 1 \end{cases}$$

Communication/Computation Overhead

- Communication overhead is negligible
- Computation overhead is low

$$\text{POTP}(K, T, SN, src\text{-}addr) = \text{Truncate}\big(\boldsymbol{HMAC}(K, T, SN, src\text{-}addr)\big)$$

Energy Consumption

- Use the benchmark result in the TI report
- 128-bit key
  - Hardware: $E_{PhyAuth} \approx 1.1\ E_{MIC}$
  - Software: $E_{PhyAuth} \approx 0.8\ E_{MIC}$

Security Analysis

- **Goal**

  Inject fake packets

- **Type-1 attack**: fake POTP
- **Type-2 attack:** replay attack

  Each POTP satisfies the one-time property

- **Type-3 attack:** adversary may acquire the device-specific key

Benefits of PhyAuth

- No hardware modification
- Standard-complaint
- Software updates
- Low-intrusive
- Low-cost

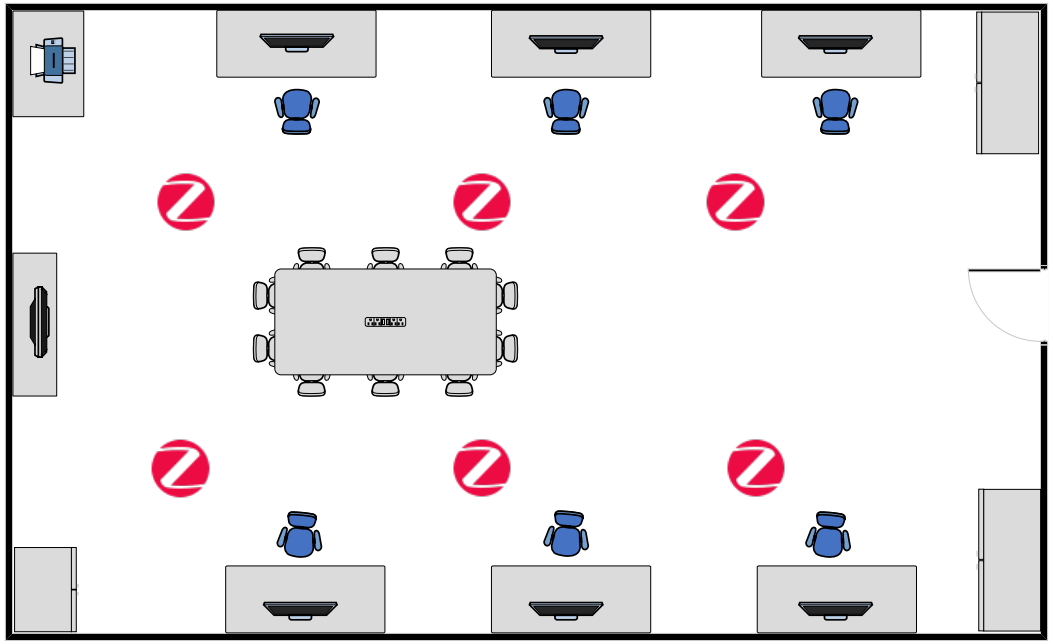
Experimental Setup

Verifier

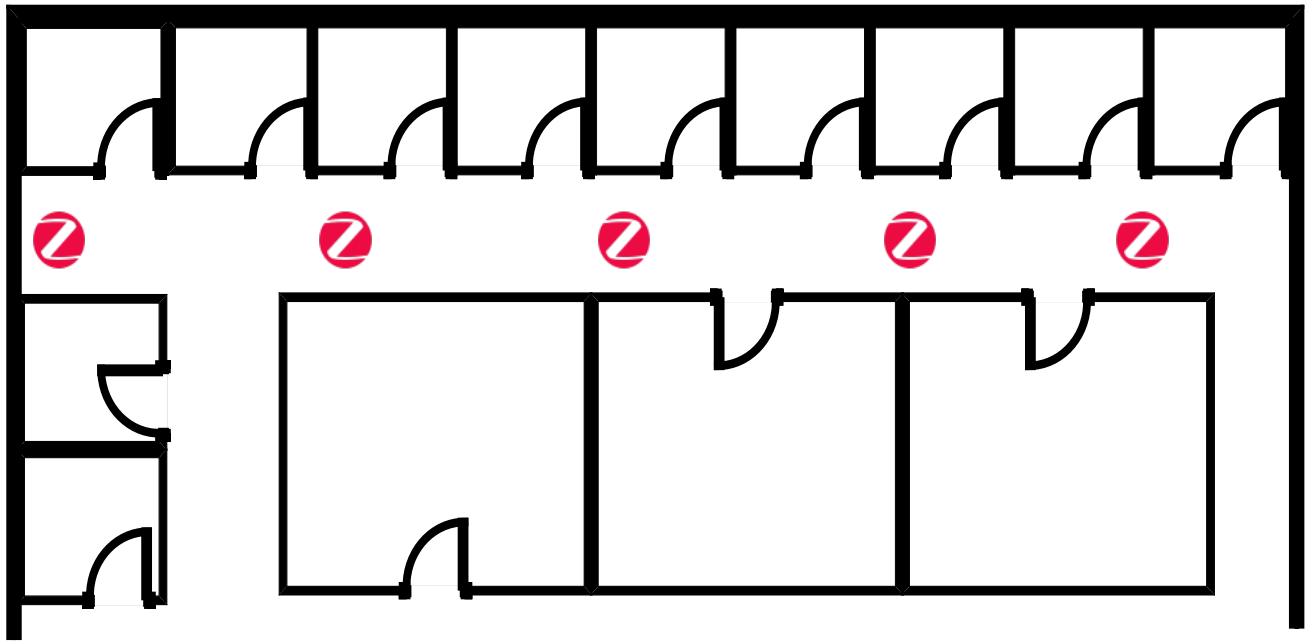
Transmitter

Receiver

Experimental Setup

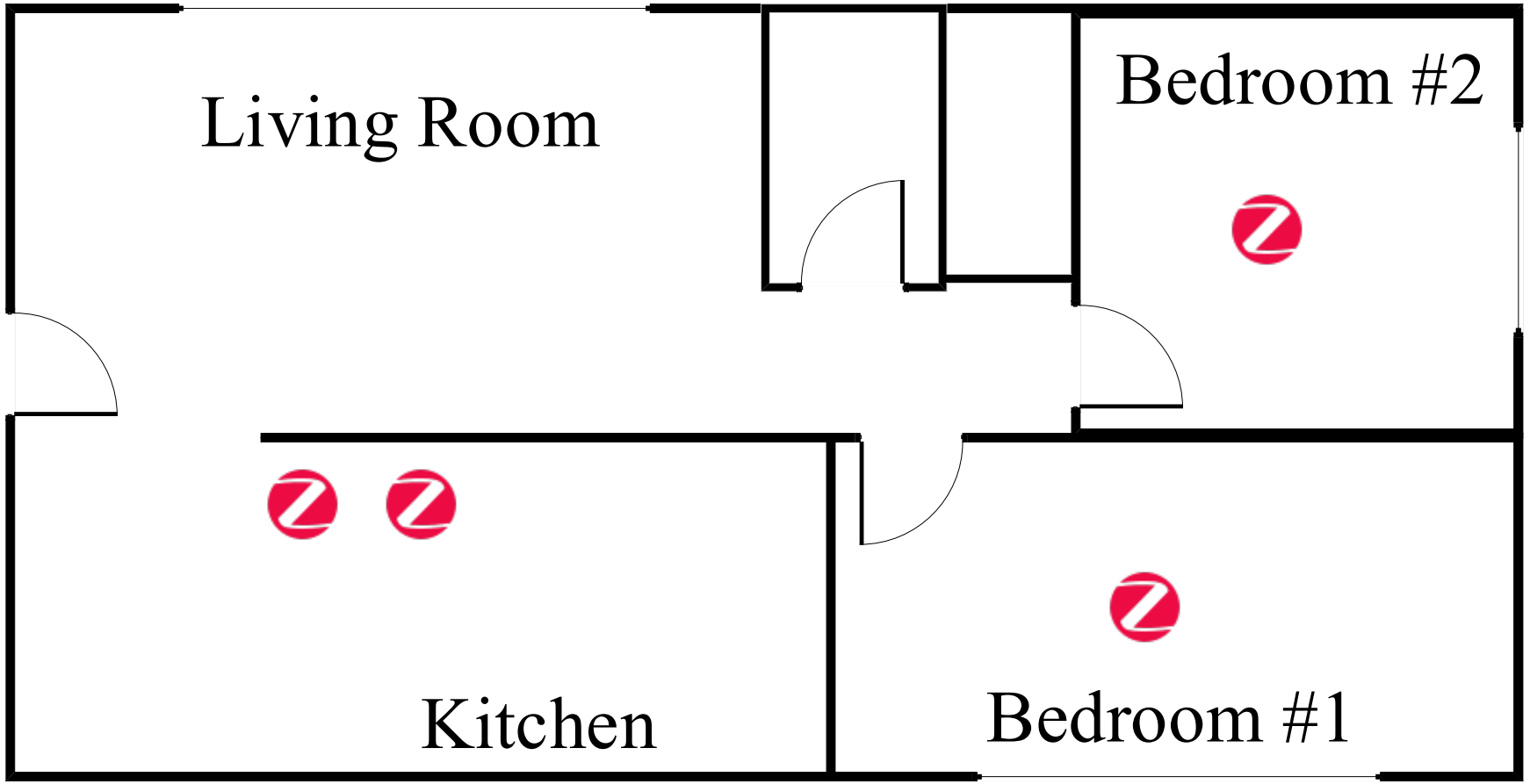


Lab



Hallway

Experimental Setup

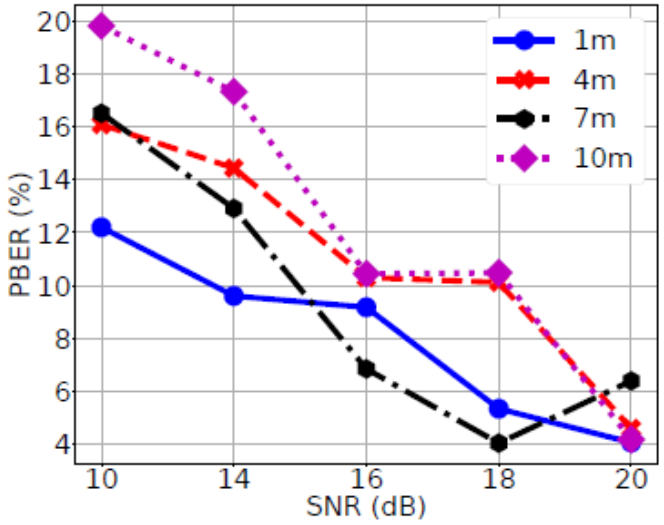


Apartment

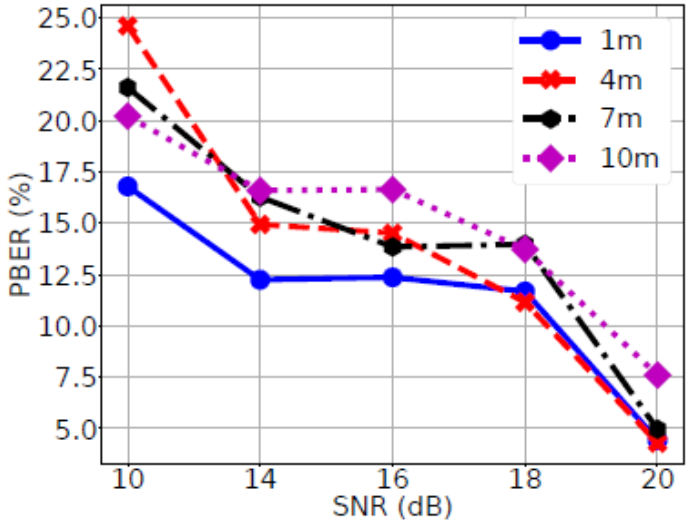
Performance Metric

- POTP-bit error rate (PBER)
- Packet error rate (PER)
- False-negative rate (FNR)
- False-positive rate (FPR)

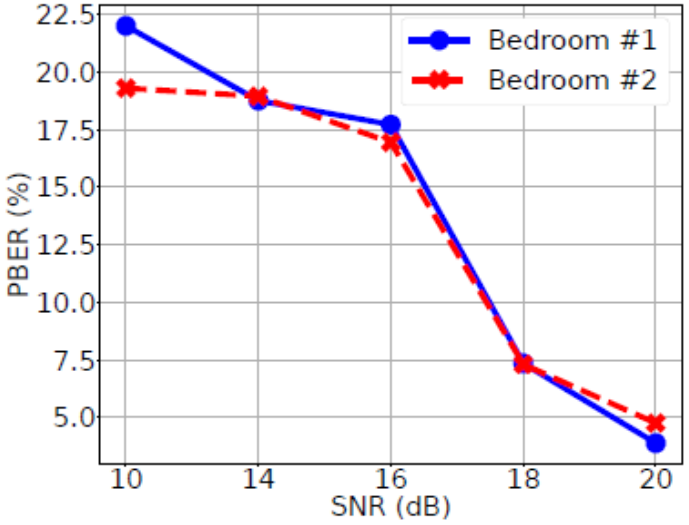
PBER Performance—VarChip



(a) VarChip at Lab

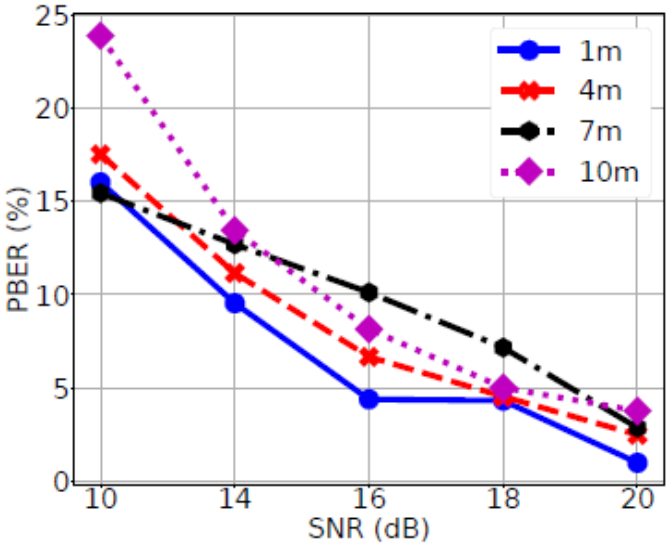


(b) VarChip at Hallway

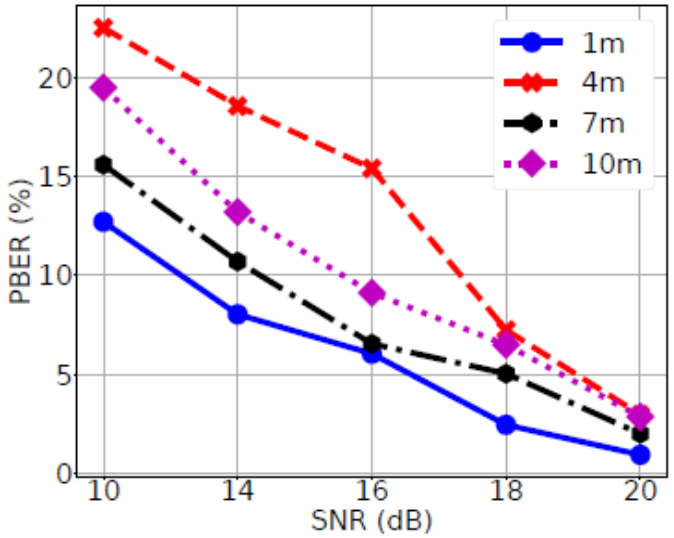


(c) VarChip at Apartment

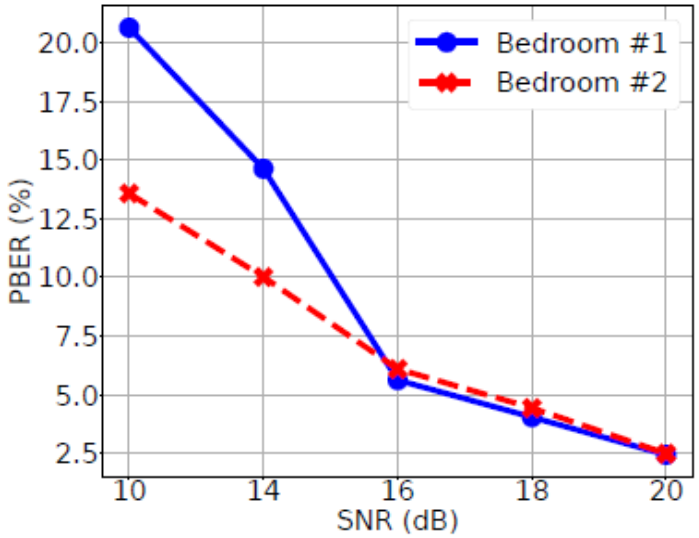
PBER Performance—VarAmp



(d) VarAmp at Lab

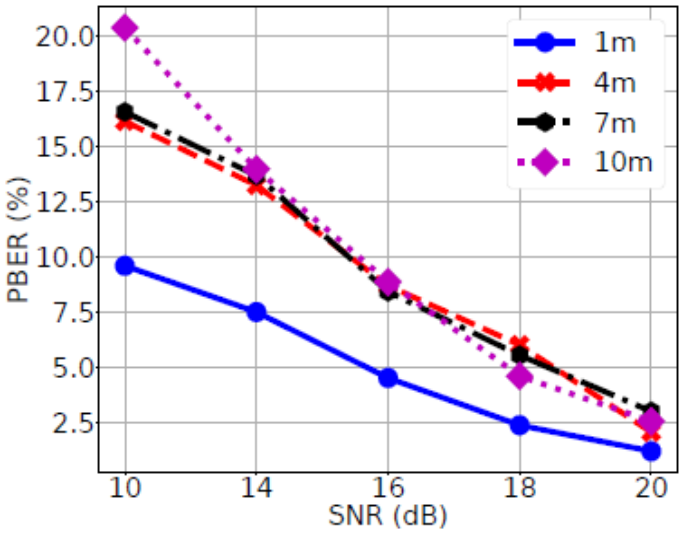


(e) VarAmp at Hallway

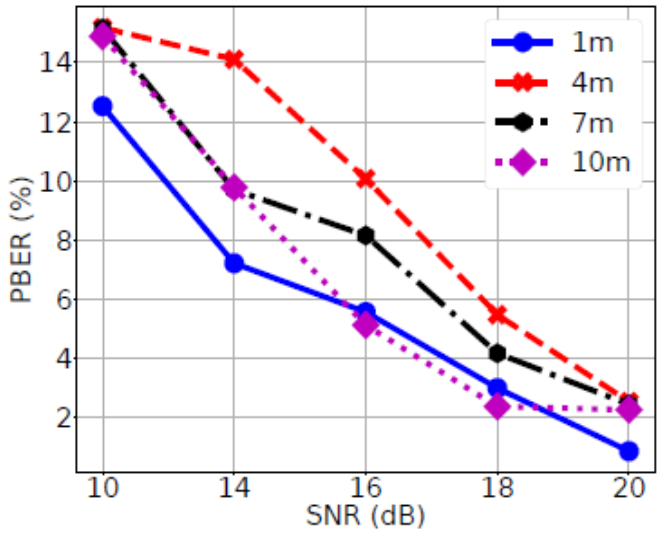


(f) VarAmp at Apartment

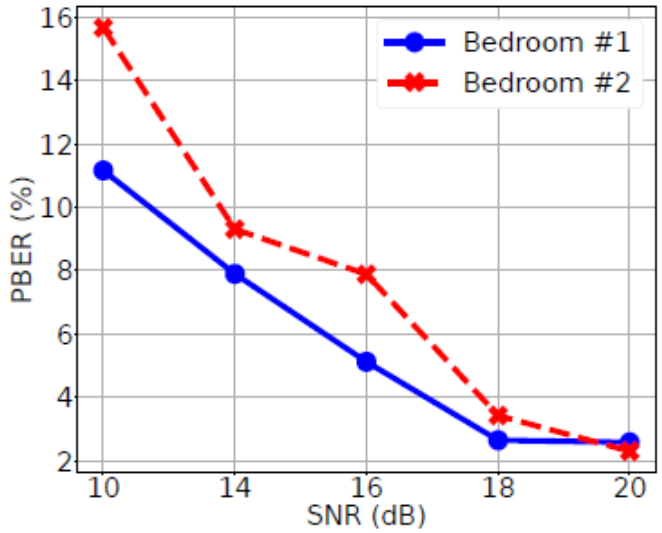
PBER Performance—VarPhase



(g) VarPhase at Lab

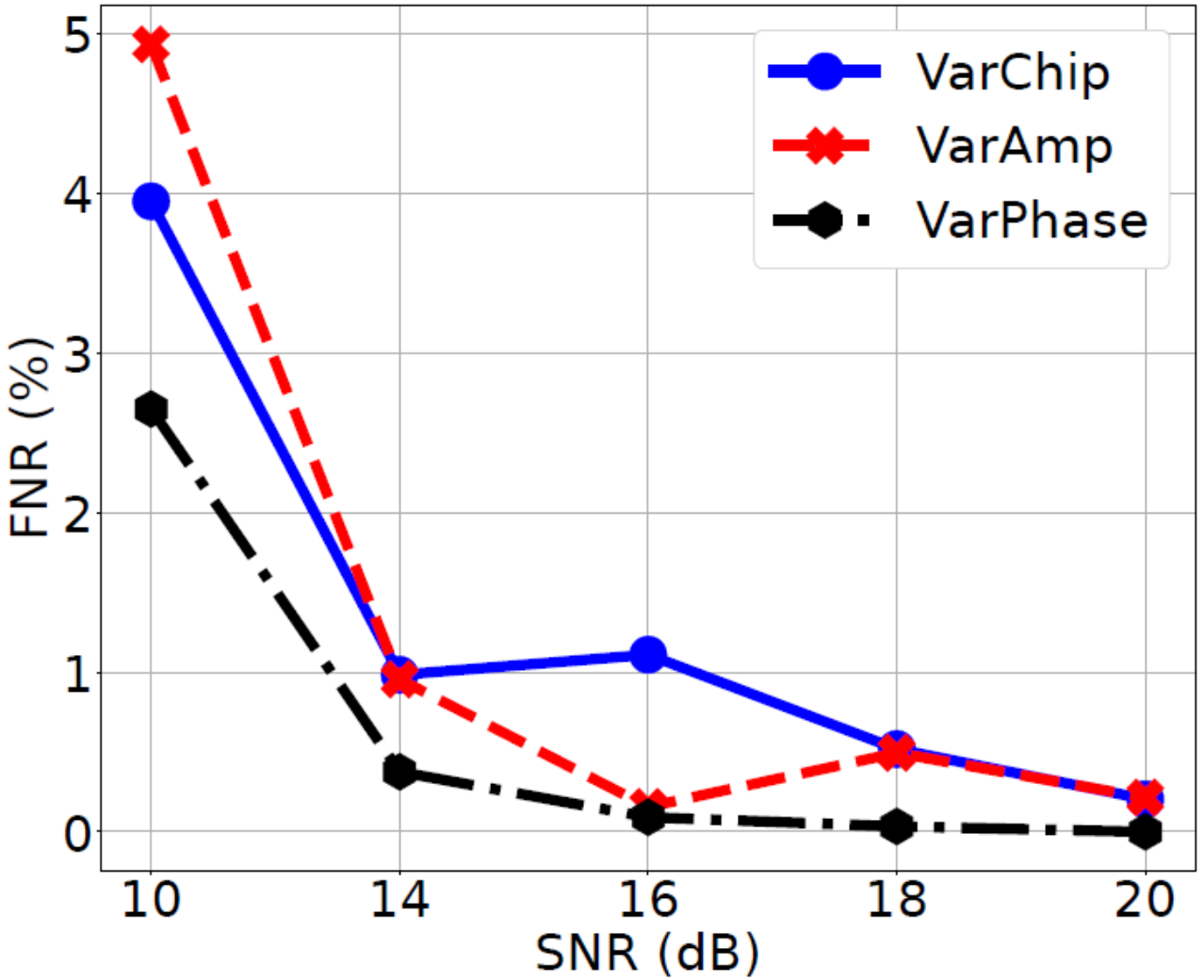


(h) VarPhase at Hallway

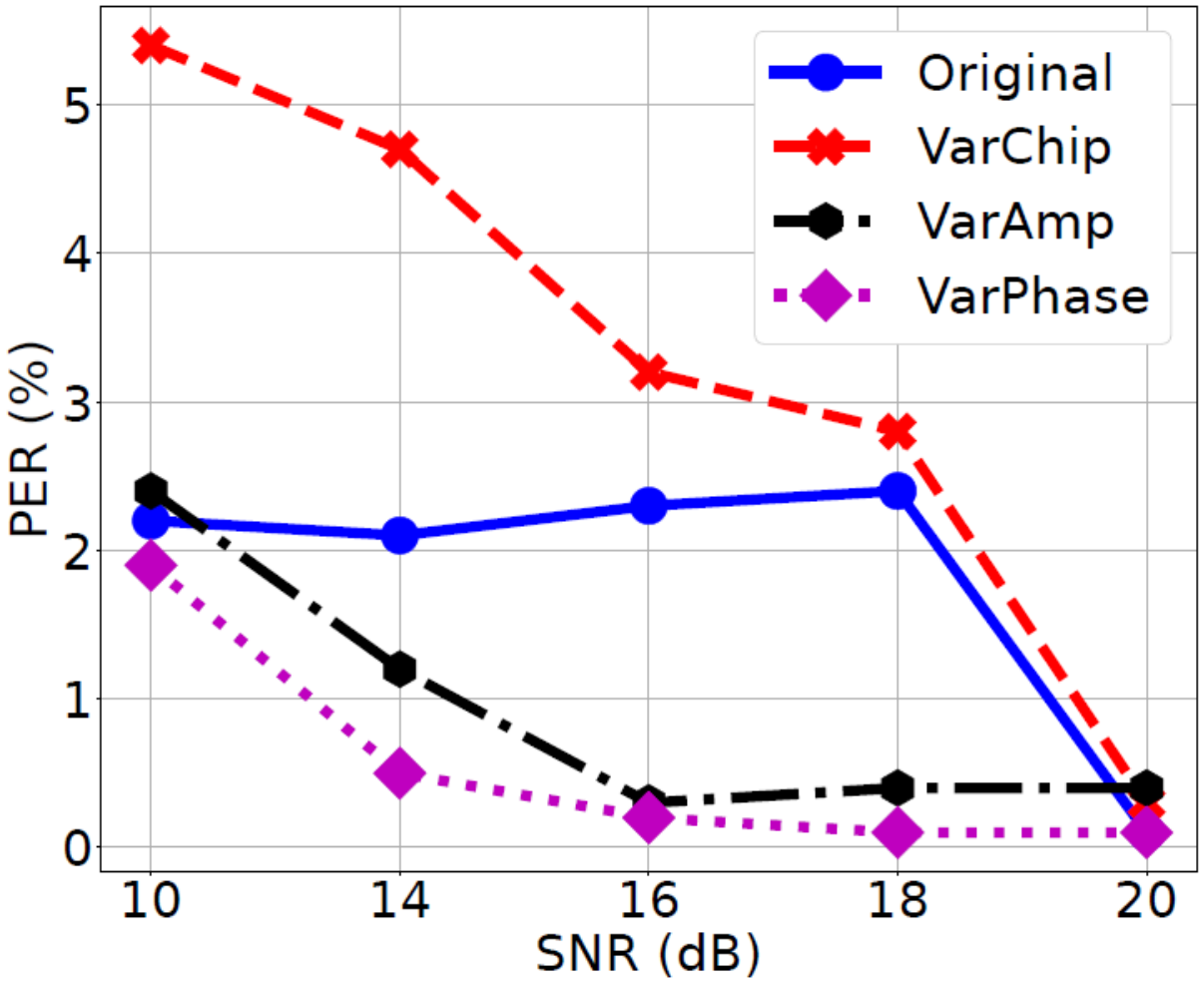


(i) VarPhase at Apartment

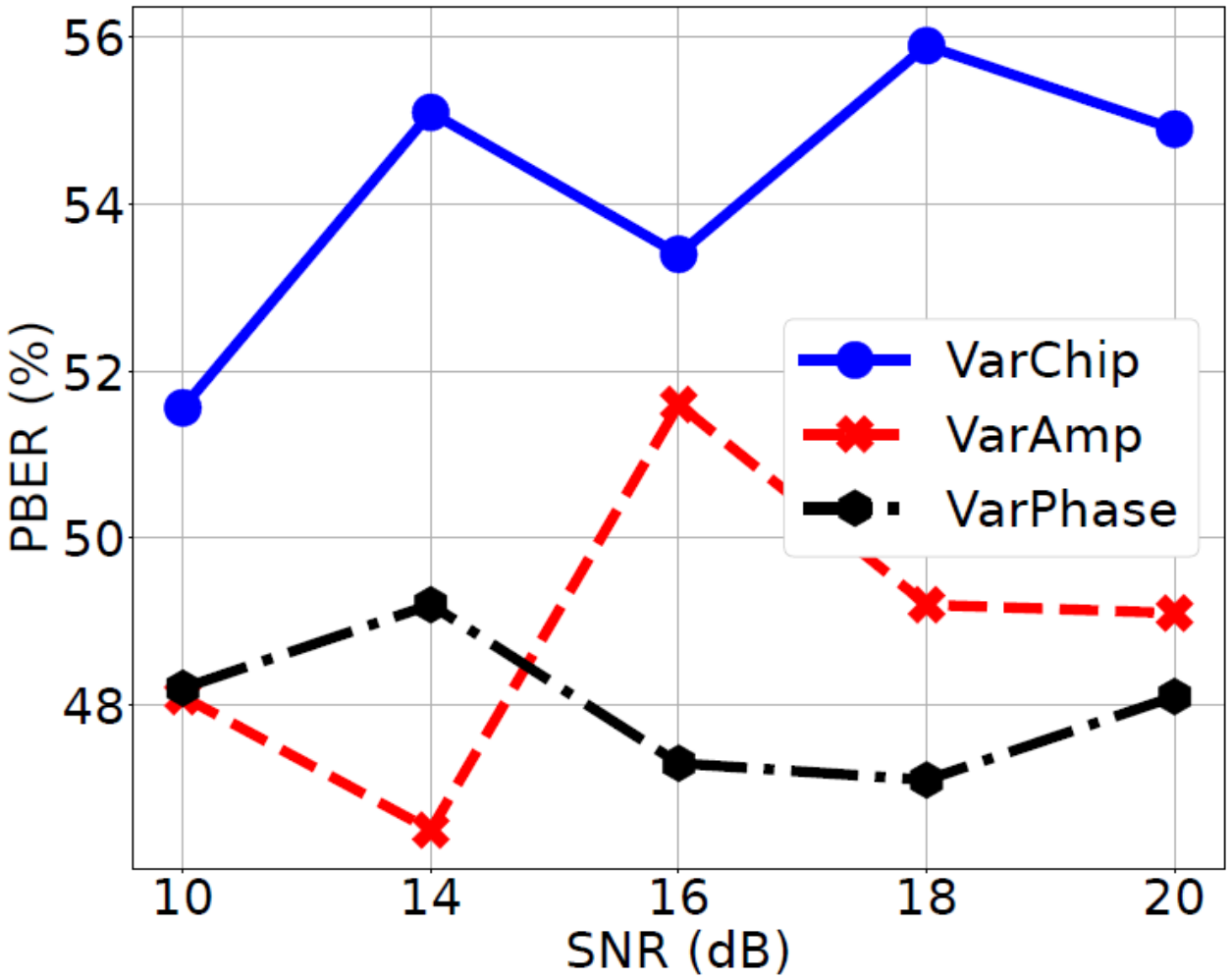
FNR Performance



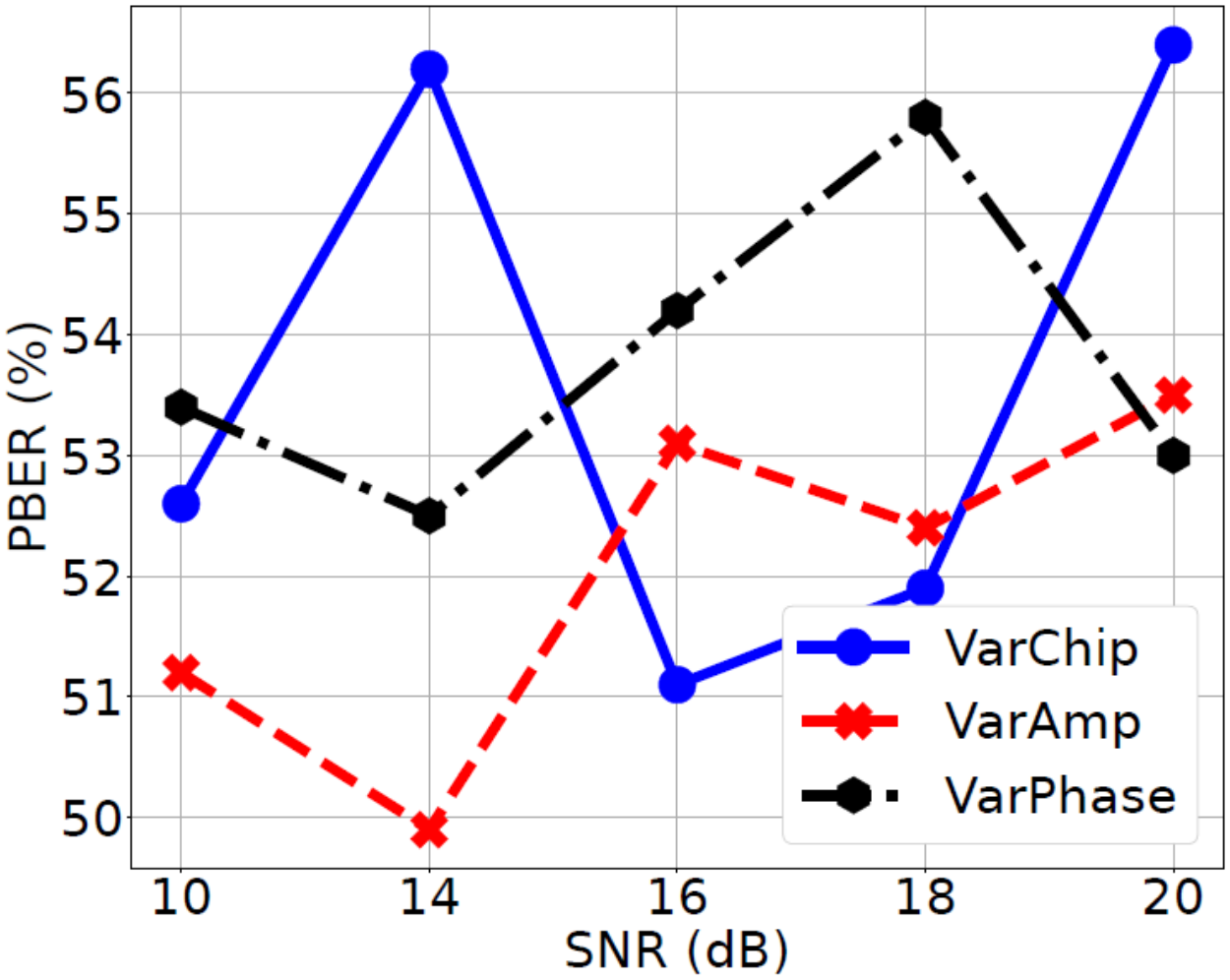
PER Performance



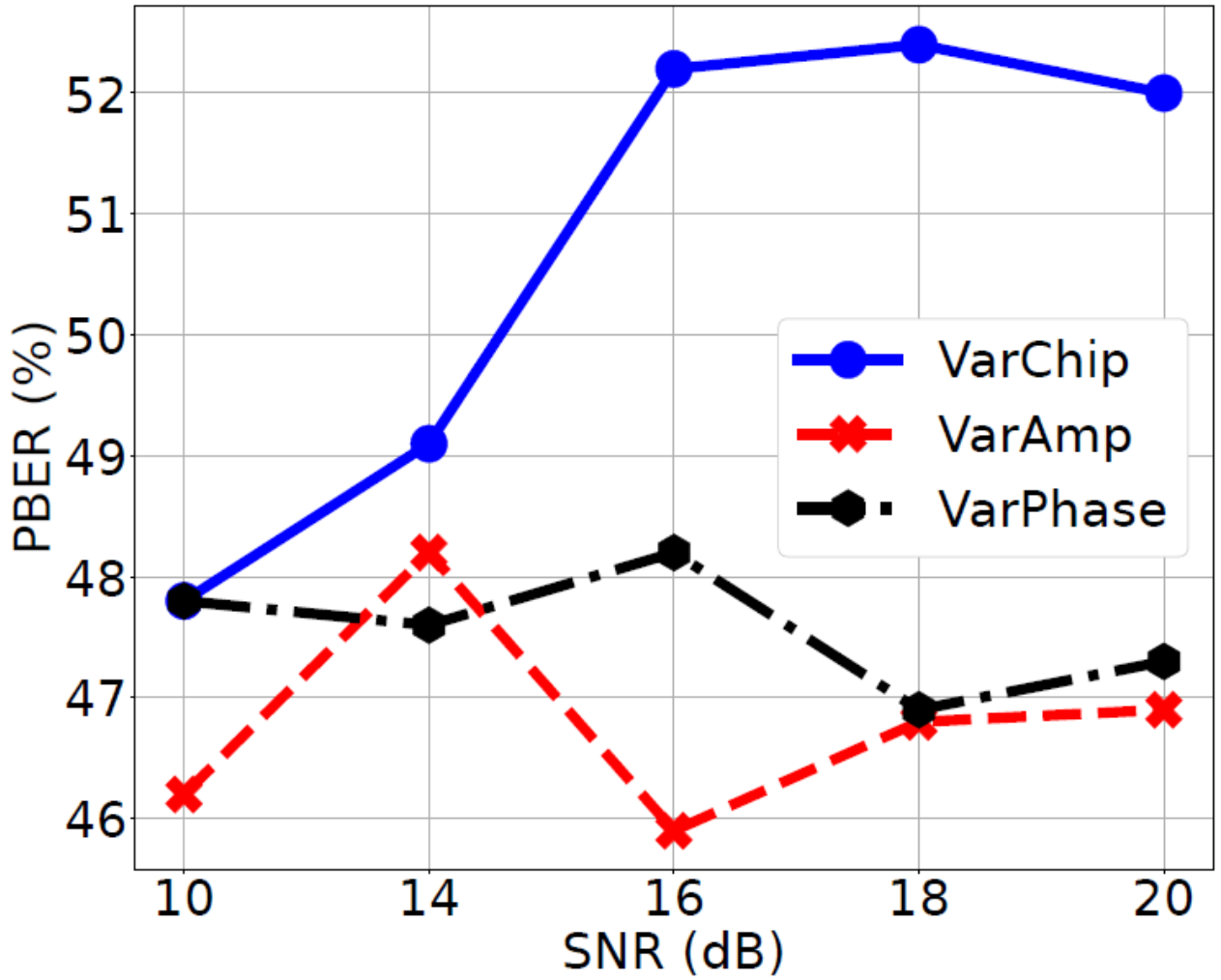
Performance under Attack—No POTP



Performance under Attack—Fake POTP



Performance under Attack—Replay POTP



Conclusion

- PhyAuth

  PHY hop-by-hop message authentication framework

- Benefits
  - ➢ No hardware modification
  - ➢ Standard-complaint
  - ➢ Software updates
  - ➢ Low-intrusive
  - ➢ Low-cost

Thank you!

Q & A?