Opportunities and Pitfalls in Securing Visible Light Communication on the Physical Layer

Jiska Classen, Daniel Steinmetzer, Matthias Hollick

Jiska Classen

Technische Universität Darmstadt
Secure Mobile Networking Lab - SEEMOO
Department of Computer Science
Center for Advanced Security Research Darmstadt - CASED

Mornewegstr. 32
D-64293 Darmstadt, Germany
Tel.+49 6151 16-25474, Fax. +49 6151 16-25471
http://seemoo.de or http://www.seemoo.tu-darmstadt.de

Physical Layer Security

- Using physical effects that are already there
- Typically more light-weight than cryptographic solutions
- Ideal for visible light communication and Internet of Things applications

VLC has different physical layer characteristics compared to WiFi.

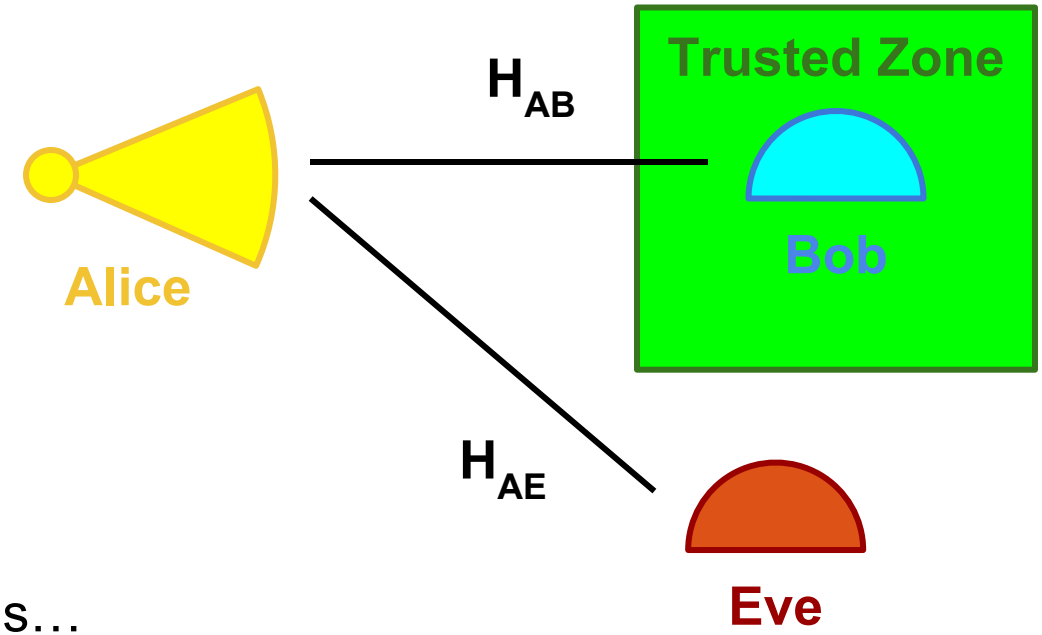
Can we use physical layer security for VLC?

How do VLC characteristics strengthen/weaken security?

Attacker Model
Examples

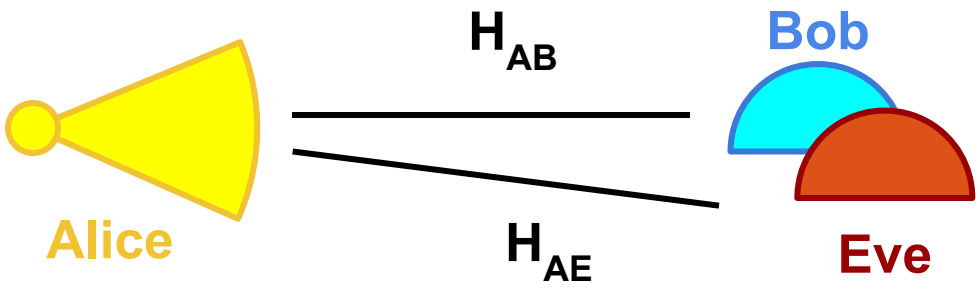
- **User failures**
  - Failure to spot an attacker within trusted zone
- **Better equipment**
  - Attacker has thousand phothodiodes
- **Additional information**
  - Attacker guesses plain-text
- **Active attackers**
  - Blockage and injection of signals

Confidentiality
Wyner's Wiretap Channel



- Channel H_{AB} is…
  - not known by Eve
  - not reproducible by Eve (often called "trusted zone")
- Channel difference can be used to encode confidential information

Confidentiality
Wyner's Wiretap Channel



- In practice: unknown attacker location!
  - Eve in proximity gets some information, but how much?
  - Assumption that Eve is not within trusted zone.

Confidentiality
Wyner's Wiretap Channel

- **User failures**

  Failure to spot Eve inside trusted zone,
  even though light propagates more intuitive

- **Better equipment**

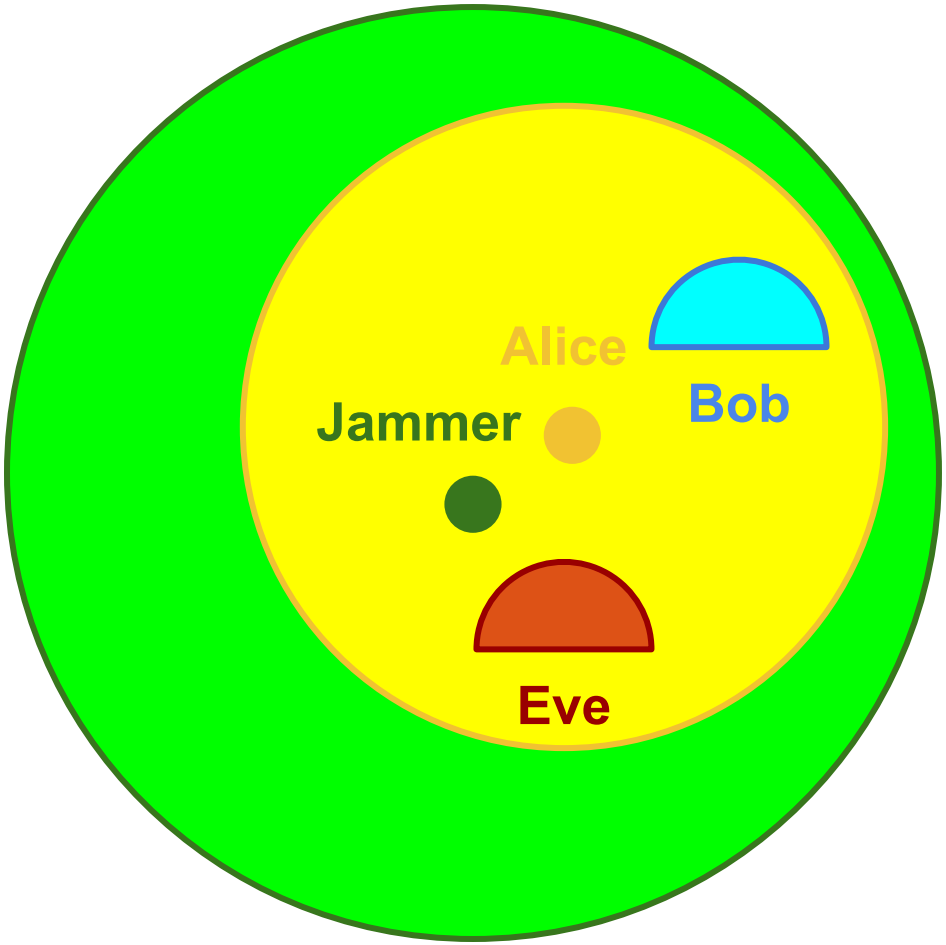
  Additional photodiodes enable Eve to receive more information,
  despite worse channels outside trusted zone

- **Additional information**

  The incoherent visible light channel H_{AB} contains only light intensity variations, no phase: easier to guess for Eve!

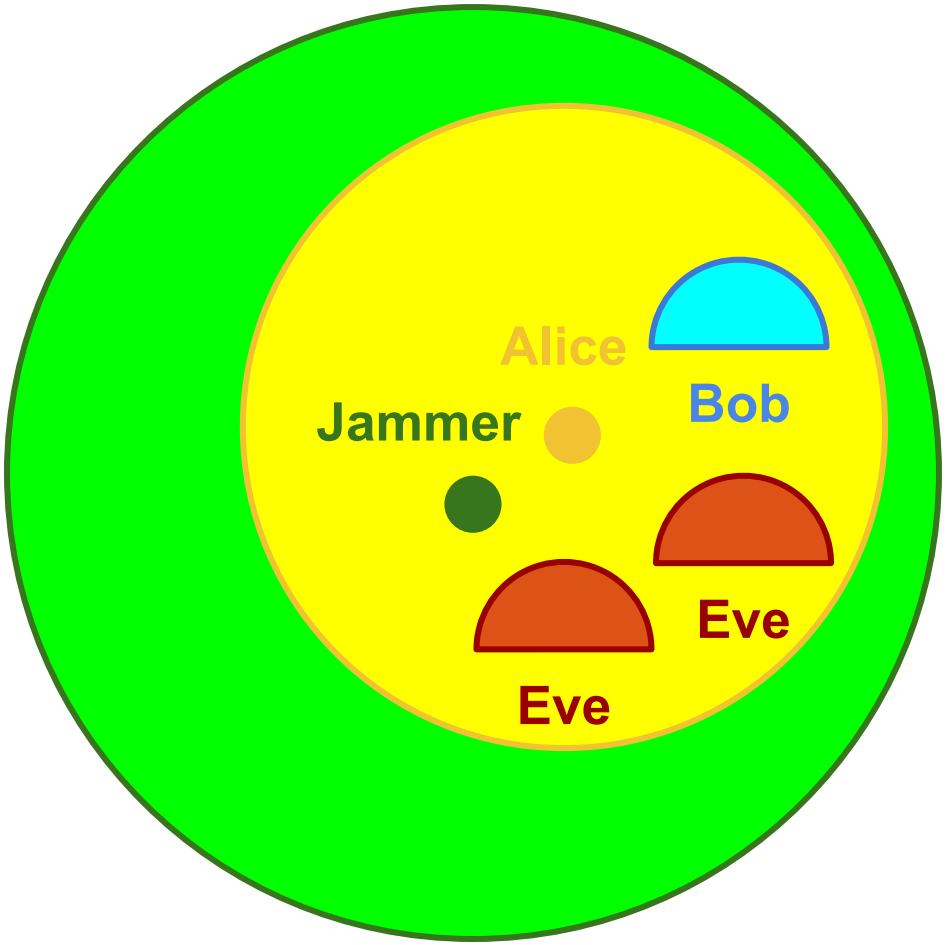
Confidentiality
Jamming

- Bob can synchronize to the pseudo-random jamming sequence and remove it
- Eve has no key to generate the jamming sequence, jamming prevents from…
  - decoding data from Alice
  - transmitting data inside jammed zone



Confidentiality
Jamming

- Eve can use multiple photodiodes to subtract the jamming
- Since the jamming is only amplitude additions, the attack becomes easier than for WiFi

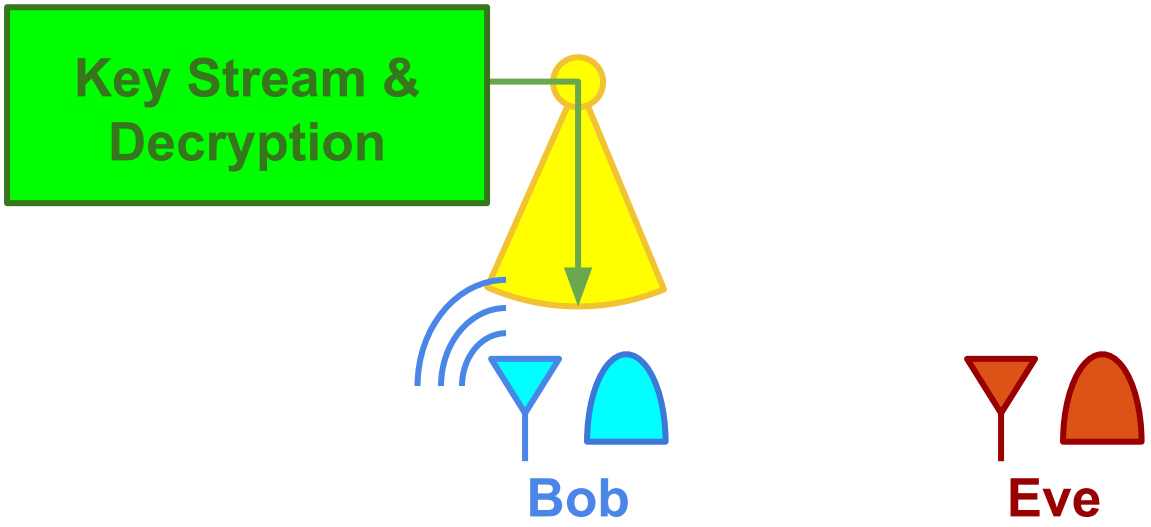


Confidentiality
Jamming

- **Better equipment**

  Additional photodiodes enable Eve to remove the jamming signal

Confidentiality
Keys



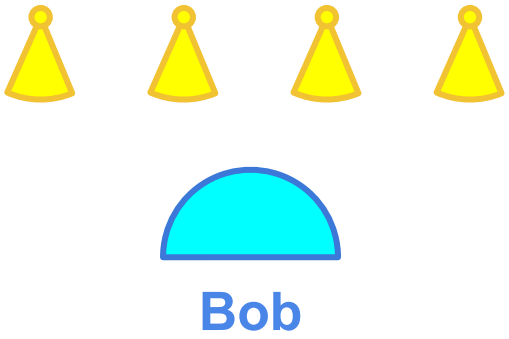
- Central instance generates random key stream transmitted over VLC
- Stream can be used as one-time pad for WiFi
- Eve's WiFi transmission range is limited to the VLC range

Confidentiality
Keys

- **User failures**
- **Better equipment**

Both can cause a VLC range that is higher than expected,
but the actual range shortage from WiFi range to VLC range is not affected

Localization and Authentication
Known Patterns



- Multiple fixed pattern transmissions enable Bob to locate himself
- Possibility to transmit data along with location information

Localization and Authentication
Known Patterns

- Attackers might inject false location information
- If Bob is not trusted, he can report a false location, because channel reciprocity is missing in VLC

Localization and Authentication
Known Patterns

? **User failures**

Users might not see attackers injecting false locations

? **Better equipment**

Additional equipment is required for attacks, but solely does not make a successful attack

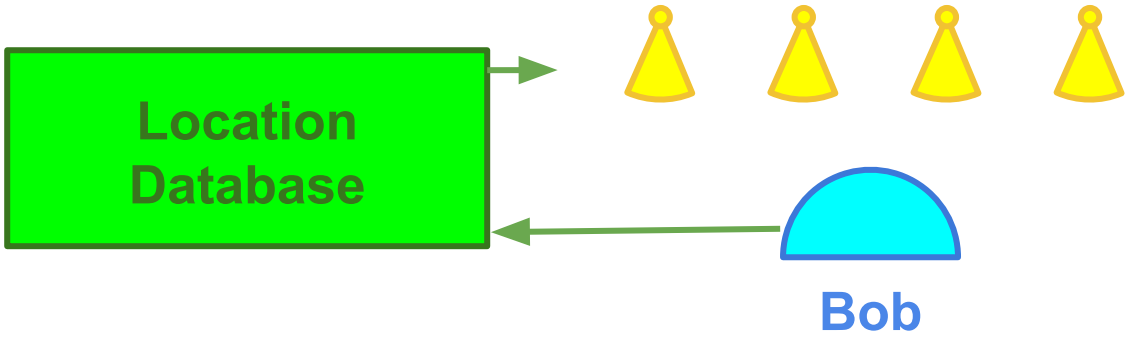
⚡ **Additional information**

Attackers knowing the pattern can report oblivious locations

⚡ **Active attackers**

Active attackers can block the localization and, with pattern knowledge, fake locations to users

Localization and Authentication
Random Patterns



- Patterns send to Bob are random
- Bob cannot compute his position, but needs to report measurements to a central instance doing the computation

Localization and Authentication
Random Patterns

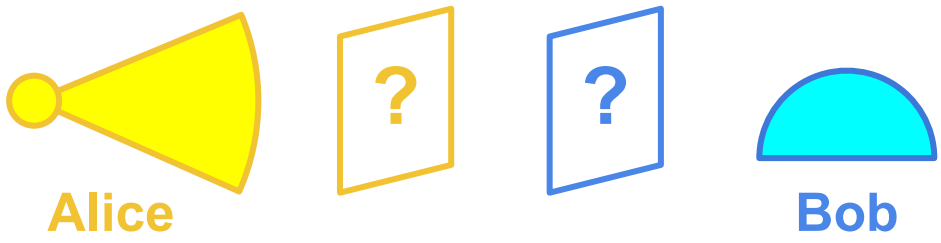
SECURE MOBILE NETWORKING

✓ Randomness successfully prevents the aforementioned attacks

? **Better equipment**

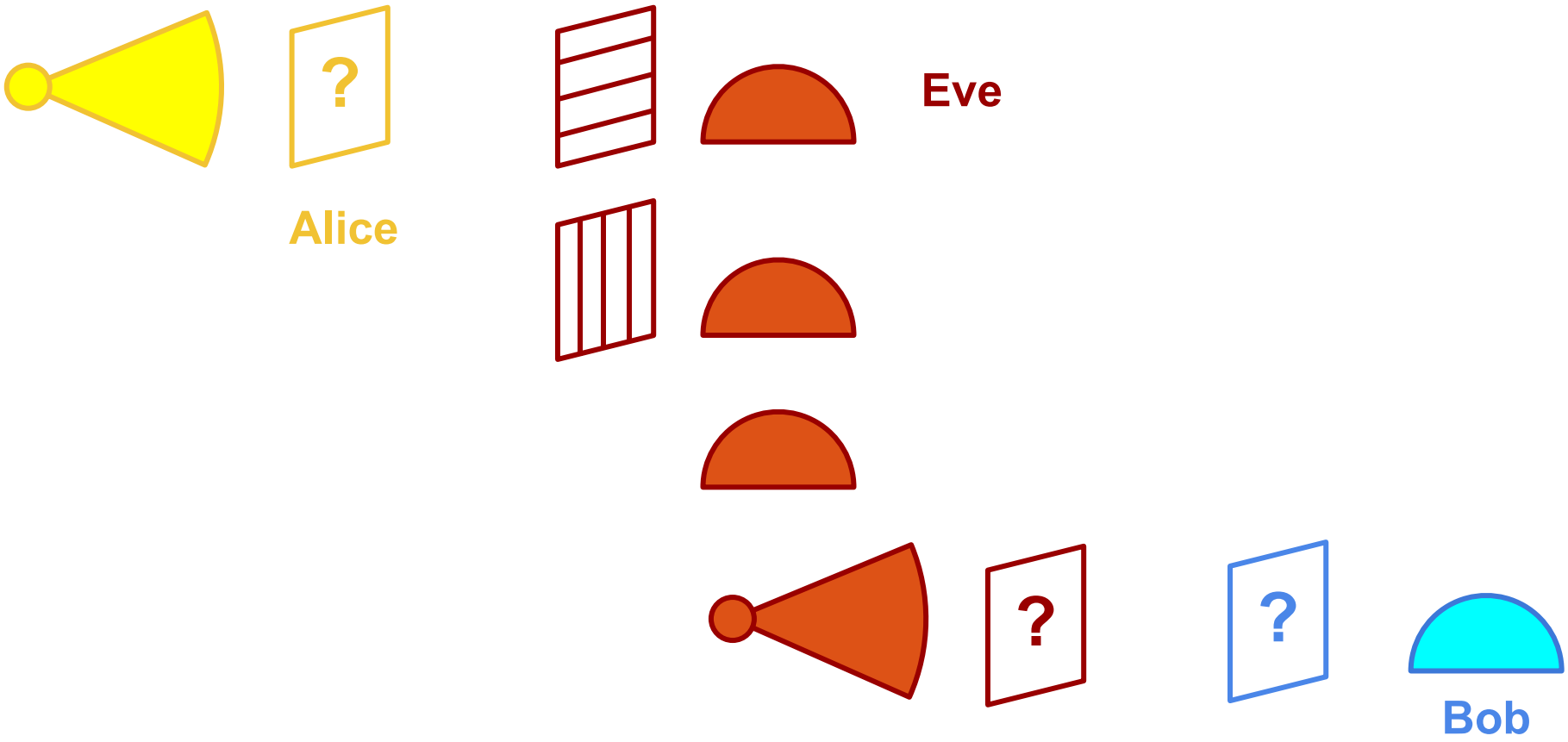
Multi-antenna attackers might still extract the location pattern and replay it, which requires the addition of distance bounding

Integrity
Polarization



- Alice and Bob vary their polarization filter by a shared pseudo-random pattern
- Only if the patterns match, the transmitted information can be reconstructed

Integrity
Polarization



- Eve can measure the polarization pattern and inject her own signal

Integrity
Polarization

- **Better equipment**

  Attackers with additional hardware can extract polarization information, hence can decode signals

- **Active attackers**

  Active attackers can even inject signals

Overview

	Wiretap channel	Jamming	Keys	Known patterns	Random patterns	Polarization
User failures	⚡	✓	?	✓	✓	✓
Better equipment	⚡	⚡	?	?	?	⚡
Additional information	⚡	✓	✓	⚡	✓	✓
Active attackers	✓	✓	✓	⚡	✓	⚡

Conclusion

Can we use physical layer security for VLC?

How do VLC characteristics strengthen/weaken security?

- Schemes that do not require channel reciprocity can be adapted
- Missing phase information weakens approaches
- Better range estimation by users strengthens approaches
- WiFi attacks also apply to VLC physical layer security