The Spy Next Door: Eavesdropping on High Throughput Visible Light Communications

Jiska Classen
Secure Mobile Networking Lab
TU Darmstadt, Germany
jclassen@seemoo.tu-darmstadt.de

Joe Chen
Rice Networks Group
Rice University, Houston, USA
joe.chen@rice.edu

Daniel Steinmetzer
Secure Mobile Networking Lab
TU Darmstadt, Germany
dsteinmetzer@seemoo.tu-darmstadt.de

Matthias Hollick
Secure Mobile Networking Lab
TU Darmstadt, Germany
mhollick@seemoo.tu-darmstadt.de

Edward Knightly
Rice Networks Group
Rice University, Houston, USA
knightly@rice.edu

ABSTRACT

Wireless networks based on visible light communication (VLC) are often considered to be resilient to eavesdropping by design, since light cannot penetrate most walls and objects. In this paper, we experimentally study the ability of a VLC eavesdropper to intercept and decode a transmission even while being outside of the direct beam. We design a testbed using software defined radios (SDRs) and evaluate different VLC eavesdropping scenarios. We find that a small gap under a door can be sufficient for an eavesdropper to decode high-order modulated (DCO-OFDM 64-QAM) reflected signals outside of a room. Likewise, neither Victorian keyholes nor window coatings provide any significant protection against information leakage to the outside. Furthermore, eavesdroppers located in the same room but not facing the sender can profit from reflections on walls.

1. INTRODUCTION

VLC is a technology for transmitting data from illumination sources such as light-emitting diodes (LEDs) to receivers such as photodiodes and cameras. Some common application scenarios include repurposing illumination sources for wireless LANs [3], vehicular networks [6], and mobile health-monitoring [13].

It is often assumed that, because light signals cannot penetrate walls, VLC provides inherent security advantages compared to radio [10]. In this paper, we experimentally study the resilience of VLC systems to eavesdropping in indoor settings representing WLANs and device-to-device communication scenarios. We consider passive attackers hiding in non-line-of-sight (NLOS) paths that attempt to intercept the communication stream by exploiting the structure of the physical environment, including small-scale material gaps, reflective materials, and transparent materials. In particular, we make the following contributions.

First, we define a system and attacker model for VLC WLANs. In this model, an attacker is not successful merely by detecting if light is on or off, as would be the case with on-off keying. Instead, higher order modulation based on orthogonal frequency-division multiplexing (OFDM) must be decoded. To avoid being detected and blocking the main signal beam, the attacker must exploit secondary and non-ideal propagation paths and contend with degraded signal-to-noise ratio (SNR).

Second, we implement a SDR testbed comprising wireless open-access research platform (WARP) boards interconnected with off-the-shelf LEDs and photodiodes. We use this to test different scenarios that allow an eavesdropper to spy on a visible light communication link that is assumed to be secret based on both directionality and light's inability to penetrate most obstacles. These configurations feature a variety of physical materials and geometric constructions representing real-world eavesdropping scenarios: through floor-to-door gaps, keyholes, and partially covered windows as well as via NLOS reflections inside a room.

Finally, we perform an extensive measurement study using the aforementioned testbed and draw the following conclusions. Nearby attackers as the "spy next door" can often intercept VLC signals, potentially revealing information on personal habits in smart-home applications, or even sensitive health data. Indoors, reflections on walls are sufficient for eavesdropping, affecting Internet of Things (IoT) applications.

The remainder of this paper is structured as follows. We describe our testbed and security assumptions in Section 2. Experiments in different evaluation scenarios are conducted in Section 3. In Section 4, we discuss related work and finally conclude this paper in Section 5.

2. TESTBED AND EVALUATION SETUP

In this section, we describe the modulation scheme that the eavesdropper must decode along with the hardware and software setup and testbed. Moreover, we present the system and adversary models.

VLCS'15, September 11, 2015, Paris, France.

DOI: http://dx.doi.org/10.1145/2801073.2801075.

2.1 Modulation

Typical light sources have a large beamwidth, since they are installed to illuminate the environment. Unlike legacy radio WiFi systems, VLC signals feature a distinct area of reception and do not encode phase information [6]. Furthermore, VLC is different from optical communication with lasers, in which coherent signals propagate on a narrow path from sender to receiver, thereby restricting eavesdropping to a few locations [7].

We use a white LED as a sender and therefore do not employ color-shift keying (CSK) as defined in 802.15.7 [2]. Instead, we employ DCO-OFDM, similar to the setup in [11], in order to re-use components of the 802.11 baseband and efficiently use the limited bandwidth of our LED, which has a linear operation range of only 2 MHz. Since we modulate light intensity of incoherent light, there are two restrictions: first, light intensity can only be positive in contrast to an electromagnetic field, and second, incoherent light has no consistent carrier phase that could be used for modulation. Therefore, symbol representation must be real-valued and positive. DCO-OFDM meets these requirements by using only half of the total subcarriers to obtain a real-valued OFDM signal and then adds a constant DC offset to produce a positive intensity.

2.2 Hardware setup

We construct a SDR testbed for VLC based on WARP v1.2 [1] as well as an array of white LEDs as the sender (Bridgelux BXRA-40E0950-B-03) and a photo diode as the receiver (LEC-RP0508). WARP is a SDR for rapid prototyping wireless communication systems in combination with MATLAB. By using the WARPLab FPGA design, a computer encodes the signals and triggers the transmission on multiple connected WARP boards. This WARP-based setup is very flexible and can be extended to drive multiple senders and receivers simultaneously.

We extend the WARPs, which typically outputs legacy WiFi carrier signals, with an analog boards interfacing arbitrary baseband signals as required for DCO-OFDM, which is shown in Figure 1. This setup provides a sampling rate of 40 MHz that is sufficient for transmission with LEDs that typically have a modulation bandwidth of 2-3 MHz. We modulate 128 subcarriers, but only 64 carry the data to obtain a real-valued OFDM output from the analog boards. A DC offset is added by another circuit, whose voltage can be adjusted to enhance the optical power. The driver circuit converts voltage to a current, changing LED brightness, thus modulating the signal onto the LED's brightness. At the receiver, the photodiode converts light to current, which the VLC receiver amplifies and the driver circuit converts to voltage.

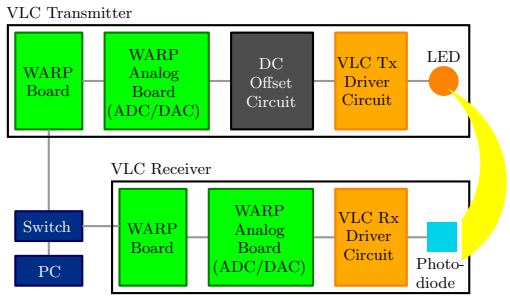


Figure 1: Schematic overview on the testbed system.

2.3 Adversary model

We consider that Alice transmits to Bob using VLC. Alice attempts to prevent eavesdropping by relying on visible light's directionality and blockage characteristics. However, Eve aims to undermine this privacy and eavesdrops on Alice's transmission. We consider NLOS positions where Alice and Bob might not expect eavesdroppers because they are considered to have poor or no reception. Outside of the room, Eve takes advantage of the gap underneath a door, keyholes, and windows. Inside the room, she can rely on environmental reflections to eavesdrop, even if she is not directly inside the light beam. In all scenarios, we assume that Bob is near the reflector or opening but not blocking the signal to Eve. We use Eve's bit error rate (BER) to quantify the success of attacks. In our experiments, no error coding is used, hence we assume that Eve can still decode signals with a BER lower than 10%. Yet, as long as the BER stays below 50%, Eve receives parts of the conversation which can be sufficient to reconstruct the message.

Note that the modulation scheme is important for successful eavesdropping—since Eve has a potentially worse path to Alice than Bob, she might not be able to decode information that is still received by Bob. While Eve intuitively is able to infer whether a light is on or off through a door gap from a large distance, we evaluate if this is sufficient or not in many scenarios for decoding higher modulation order signals.

3. EVALUATION

Each experiment is conducted with 100 repetitions to determine the median and confidence bounds. Boxplots represent the 25^{th} and 75^{th} percentiles using a box while the whiskers extend to the non-outliers. We vary sender and receiver positions and place obstacles in between as described in detail in the following.

3.1 Door gap eavesdropping

In the following, we examine if eavesdropping based on floor reflections from a 4.83 x2.73 m room is possible. Alice, having a 37° cone slightly focusing her light, is placed on a chair facing a door while Eve is located outside the room at the door's center on the ground, hence she is not facing Alice directly but exploiting reflections, as depicted in Figure 2. We find that Eve's location is optimal at 30 mm distance from the gap.

First, we record a regular receiver baseline with an open door. Then we measure the optimal scenario for Eve using

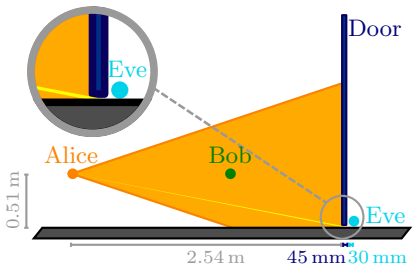


Figure 2: Eavesdropping setup through a door gap.

mirrors as well as typical flooring materials listed in Table 1. Our floor samples have a limited size, so we first inspect the influence of reflector sizes in Section 3.1.1. The original flooring is a gray carpet leaving a 15 mm gap between the door and the floor. When testing with different materials, the gap size narrows based on the thickness of the material under test, so we investigate the impact in Section 3.1.2. Afterward, we focus on materials with clear grooves and surface structures in Section 3.1.3. Finally, we cross-compare different flooring materials and their effectiveness for eavesdropping in Section 3.1.4.

3.1.1 Reflection zone

We measure the impact of reflection zone size in the following setup: Eve is located on top of a mirror in 30 mm distance to the door. The mirror is moved inside centimeter-wise towards the transmitter, Eve's distance to the door is 3 cm in all experiments. Since the original carpet is a very bad reflector (which will be shown in Section 3.1.4), the small-sized floor samples give us an upper bound on the BERs. The measurement at 0 cm is taken at alignment with the inner surface of the door while 1 cm means that the mirror is already inside the room. As seen in Figure 3, Eve's 4-QAM BER significantly drops when the mirror is 2 cm inside the room while she requires around 5 cm to achieve a good eavesdropping performance for 64-QAM. This suggests that Eve does not need very much of the reflector to be inside of the room to eavesdrop, even for higher order modulation schemes, so she could place a small reflector underneath the door if the existing flooring material is not sufficient for eavesdropping.

To validate these findings with other materials, we use a rectangular piece of parquet with a shiny surface as a reflector and measure Eve's BER for different orientations of the parquet. As Figure 4 shows, the parquet # 11 has the lowest BER when aligning the longer side along the path towards the transmitter. This corresponds to a larger reflection zone size on the NLOS path and means that our measurements in the remainder of this paper give an upper bound BER for a room completely filled with the floor material under test.

3.1.2 Gap size

Many of the tested samples are of different thicknesses, thus altering the door gap size. To analyze if this has a significant bias on our measurement results, we raise a test layer of acrylic glass to different heights to reduce the available eavesdropping gap size and then measure the BER at each of these heights. As seen in Figure 5, a narrow gap size especially raises the BER for higher modulation orders. Hence, our measurement results give upper bound BERs for each material, which can be decreased with larger gap sizes. For Eve, this means that there is a trade-off between using the existing floor material or maliciously placing another material under the door; although the material may cause better reflections in general, the performance gains may be dwarfed by the additional losses from reducing door gap size.

3.1.3 Material surface

Intuitively, surface structures on materials block light on the way to Eve. To exclude the source of different BERs from being material differences or the size, we rotate the same squared vinyl plank # 5 with wood structure crosswise and lengthwise towards Eve—since it is squared, we are only

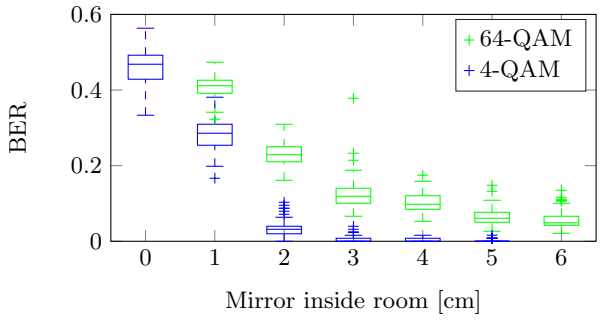


Figure 3: Moving a mirror inside.

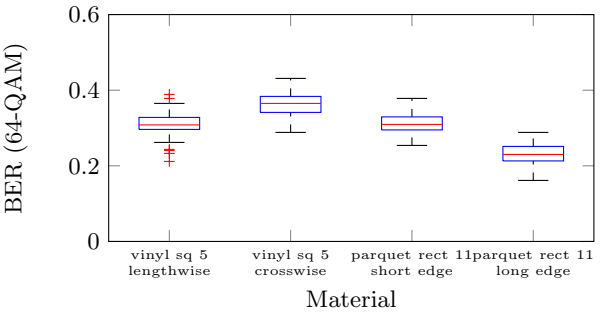


Figure 4: Different tile orientation eavesdropping performance.

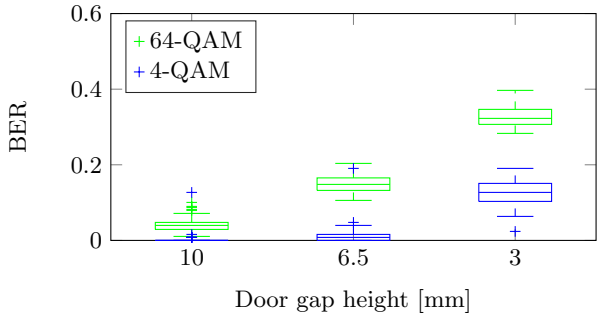


Figure 5: Acrylic glass at different heights.

changing its orientation but not the reflection zone. Figure 4 shows the difference between the orientations: even though it is the same square sized material, the mean BER drops from 36.23% to 31.01% for the lengthwise orientation of the wood structure, hence having less ripples from the vinyl on the way to Eve. This means that Eve can noticeably improve her performance by optimizing her position with regards to the flooring material's structure, even if she cannot change the flooring material itself. This difference is even larger for lower order modulation schemes (e.g. 9.81% vs. 17.35% for 4-QAM).

3.1.4 Flooring comparison

In this experiment, we compare all materials in their optimal orientation with 30 mm distance in front of the door's center front. Since the original flooring has the second worst BER, all better BERs exclusively originate from the support of the flooring materials. Note that these results are

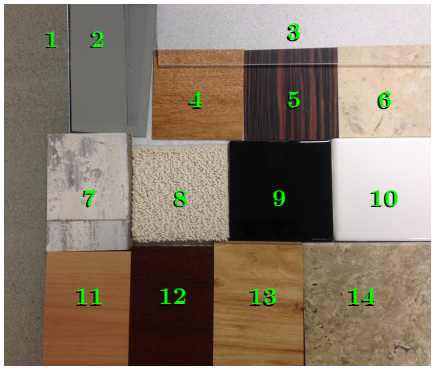


Figure 6: Floor materials.

#	Material	Height	Length	Width
0	Baseline with open door	—	—	—
1	Metal sheet	0.5 mm	750 mm	406 mm
2	Mirror	4.5 mm	302 mm	302 mm
3	Acrylic glass	5 mm	209 mm	406 mm
4	Vinyl plank "Antique Elm"	1.5 mm	100 mm	100 mm
5	Vinyl plank "Rosewood Ebony"	1.5 mm	100 mm	100 mm
6	Vinyl plank "Corfu"	1.5 mm	100 mm	100 mm
7	Laminate "Whitewashed Oak"	8 mm	126 mm	88 mm
8	Carpet "Antique Bone"	10 mm	103 mm	103 mm
9	Black shiny glazed tile	7 mm	106 mm	106 mm
10	White shiny glazed tile	7 mm	106 mm	106 mm
11	Parquet "Character Maple"	10 mm	128 mm	89 mm
12	Parquet "Mahogany Natural"	11 mm	127 mm	87 mm
13	Laminate "Middlebury Maple"	12 mm	134 mm	91 mm
14	Gray structured dull glazed tile	8 mm	147 mm	147 mm
15	Original carpet	0 mm	—	—

Table 1: Floor material sizing and description.

an upper bound on the BERs, that would be reduced by a completely filled floor of the material with a constant 15 mm gap size. In case of surface structure, we turned tiles in the optimal orientation.

The results are shown in Figure 8. We find that the non-typical flooring materials—mirrors, metal, and acrylic glass—are the best reflectors. Even at 64-QAM, their BERs stay below 5.6%. Note that the mirror in this experiment is slightly better than in prior experiments, because it is as far in Alice's room as possible, allowing it to reflect more of her signal beam towards Eve. The shiny glazed tiles are slightly better than the structured tile, but all tiles perform well for 4-QAM. Even the structured tile has a 2.8% mean BER. For laminate and parquet, the gap size was reduced by at least 8 mm respectively 10 mm. Yet, their mean BERs are 0.6% and 3.6% for 4-QAM. We assume that the other laminates and parquets are also good reflectors for larger gap sizes. A defense against VLC eavesdropping is carpet; the original carpet has 41.5% BER and the 10 mm carpet under test has 46.6% BER. This result is against intuition; even though one can see if light is on or off in the room from the position of Eve's photodiode, carpet reflections are not sufficient for decoding.

3.2 Keyhole eavesdropping

One alternative to the door gap is a keyhole, which attackers can use to eavesdrop on transmissions from outside the room. In this section, we test if Eve can eavesdrop on a transmission between Alice and Bob when Bob is in front of a door with a keyhole. We setup Alice and Eve as shown in Figure 9, with the actual keyhole aligned 51 mm from the bottom of the opening surrounded by 55 mm thick black foam, and align Eve so that her photodiode is directly behind the keyhole opening. We use a brass Victorian lock set with a keyhole depth of 26 mm. We assume that Bob is not blocking any of the signal from Eve.

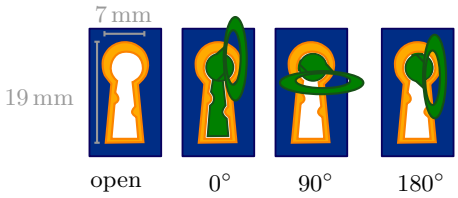
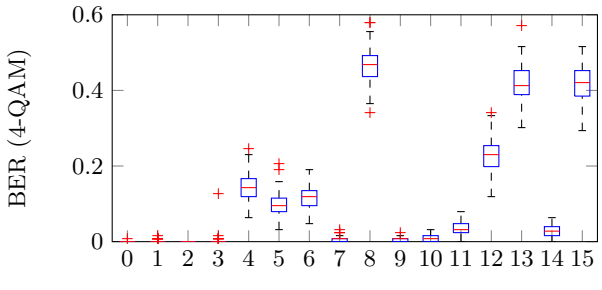
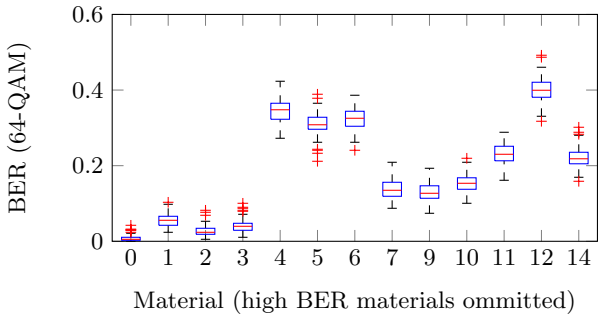


Figure 7: Eavesdropping keyhole setup.



(a) 4-QAM eavesdropping.



(b) 64-QAM eavesdropping.

Figure 8: Door gap eavesdropping on different flooring materials.

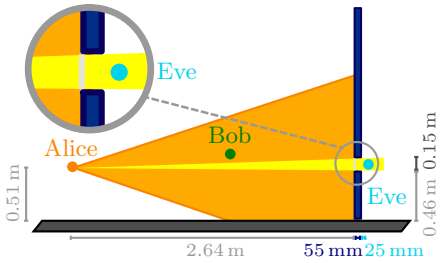


Figure 9: Eavesdropping setup for window and keyhole.

We first block the keyhole completely with foam and verify that Eve cannot decode any signal, neither 4-QAM nor 64-QAM. Afterward, we measure Eve's BER when the keyhole is open, when the key is blocking the keyhole, when the key is turned 90°, and when the key is turned 180° as illustrated in Figure 7. The results in Figure 10 show that partially blocking a keyhole has almost no effect on Eve. However, blocking the keyhole completely prevents from eavesdropping. In the 90° and 180° positions, the key handle blocks slightly different amounts of light in the path. These results suggest that, in line-of-sight (LOS), small holes are sufficient for eavesdropping.

3.3 Window eavesdropping

It is well known that windows leak information transmitted via visible light communication, but we investigate if window add-ons reduce information leakage. The experimental setup is the same as in Section 3.2, but instead of a keyhole, we mount 2 mm thick glass window pane in front of the black foam 15 x15 cm opening.

As a baseline, we first measure the 4-QAM and 64-QAM BER at Eve, without and with glass. Afterward, we attach a window film and insect screen to the glass window. The window film is an Artscape 'etched glass' film to that is advertised to both provide UV protection and create privacy. Intuitively, this material blocks a significant amount of light, since objects behind the window with this film are hard to recognize. The insect screen is a black screen intended for 4.1 mm or 4.6 mm spline sizes. Each rectangle in the screen's mesh is approximately 1.2x2 mm.

Neither the film nor the screen offer any protection against Eve when using 4-QAM; the mean BERs for all combinations stay below 1.6%. As shown in Figure 11, even using 64-QAM, these window add-ons only reduce Eve's signal quality minimally, and Eve can still decode with a small BER of a maximum 3.2% mean for combining these two modalities.

3.4 Wall eavesdropping

In smart homes and IoT application scenarios, many devices are equipped with communication interfaces and cameras. Depending on the modulation scheme, even cameras can decode VLC. In the following experiment, we analyze if devices that are nearby but in NLOS are able to eavesdrop. For this, we mount Alice on a rotator, resulting in 0.97 m height in total, and take 20 measurements in 5° steps. We replace her reflector by a narrower 17° cone instead of the 37° cone in the previous experiments to get higher directionality, which is required to further quantify where the reflections come from. Eve is positioned at the other side of the room as shown in Figure 12b and Bob is assumed to be in the direction that Alice is pointed in. The results show that the white wall and the blue painted wooden door give sufficient reflections for eavesdropping in 4-QAM when Alice is sending in the opposite direction.

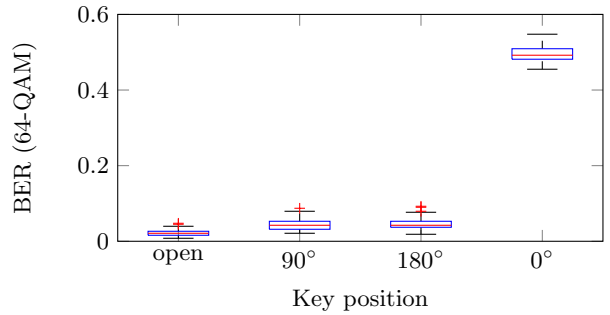


Figure 10: Eavesdropping through a keyhole.

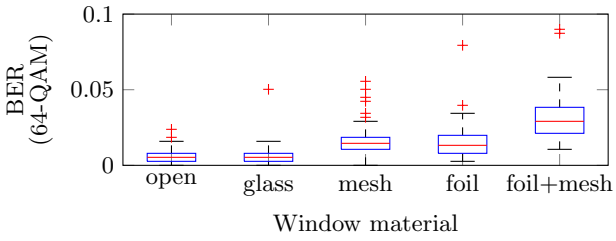
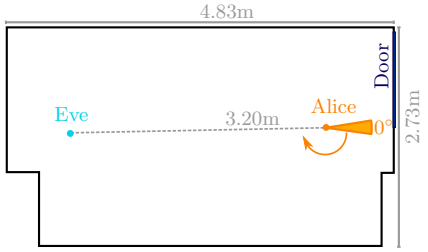
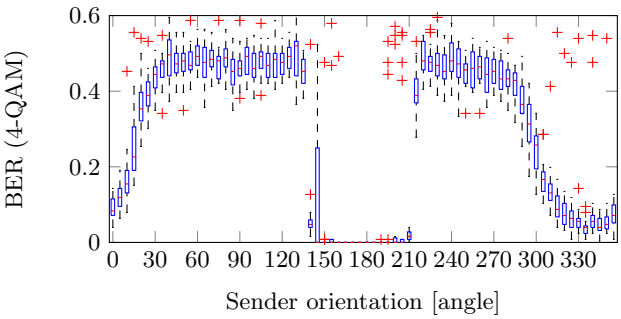


Figure 11: Eavesdropping impact of partially covering a window.



(a) Setup for measuring reflections inside a room.



(b) Eavesdropping on wall reflections.

Figure 12: Reflections within a room.

4. RELATED WORK

Recent work in VLC includes methods for increasing link rates [14], design of low-cost senders and receivers [12], and designing new VLC-based applications [3]. Yet, security and privacy in VLC applications has received limited attention.

One approach is to build security based on VLC properties. A secure barcode exchange protocol assuming that eavesdroppers have a restricted angle of view on smartphone displays is implemented in [15]. They argued that the eavesdropper cannot be at multiple positions at once, hence rotating the smartphone within the intended receiver's angle of view helps against eavesdropping. Furthermore, as in legacy WiFi frequencies, VLC can also be used to establish physical layer security. Since VLC channels are non-reciprocal and the incoherent light of an LED has no phase, most WiFi ap-

proaches cannot be adapted into VLC. There is theoretical work on null-steering [8] and friendly jamming [9].

In [7], optical laser communication eavesdropping has been studied, which has the challenge of not blocking the intended receiver, but is restricted to locations close-by a narrow beam. Old cathode-ray tube (CRT) screens emit light by raster-scanning pixels and changing the intensity. Hence, a fast photodiode can eavesdrop screen contents even from wall reflections [4]. Though, CRT screens are not optimized for high throughput VLC applications. CRTs can also be eavesdropped using side-channel EM-waves [5]—in contrast, we directly eavesdrop on the visible light and not on side-channel emissions produced by the communication devices.

5. CONCLUSIONS

One may suppose that visible light communication is secure by design because it does not penetrate most walls and obstacles. In this paper, we have shown that eavesdropping on VLC from outside of a room is not only feasible but also implementable in multiple ways: using a door gap, a keyhole, or a window. Assuming an IoT scenario, attackers controlling a single device even in the room next door can spy on communication—or conventionally hide eavesdropping devices in the flower pot next to a window and so on. DCO-OFDM on lower modulation schemes shows almost no BER at Eve for most of the attack scenarios discussed in this paper, and higher order modulation schemes are still decodable at Eve with a relatively low BER, which will be further reduced by coding schemes.

In order to make a room VLC secure against eavesdropping, we recommend poor reflectors such as carpet, modern key locks, and small door gaps. Yet, blocking a window with a privacy film offers almost no protection, although it is hard to see through it. Even from inside of the room, Eve can take advantage of reflections from everyday objects and walls to eavesdrop from outside of the main signal beam.

Acknowledgments

This work was supported by the German Research Foundation (DFG) within the project CROSSING, by the German Federal Ministry of Education and Research (BMBF) within EC SPRIDE, and the Hessian LOEWE excellence initiative within CASED. This research was also supported by Cisco Systems, Intel, the Keck Foundation, and by NSF grants CNS-1444056, CNS-1126478 and CNS-1012831.

6. REFERENCES

[1] WARP Project, http://warpproject.org.

[2] *IEEE standard for local and metropolitan area networks—part 15.7: Short-range wireless optical communication using visible light.* Std 802.15.7, 2011.

[3] *Proceedings of the 1st ACM MobiCom Workshop on Visible Light Communication Systems*, New York, NY, USA, 2014. ACM.

[4] M. G. Kuhn. Optical time-domain eavesdropping risks of CRT displays. In *IEEE Symposium on Security and Privacy, Proceedings.*, 2002.

[5] M. G. Kuhn. Eavesdropping attacks on computer displays. *Information Security Summit*, 2006.

[6] Cen B. Liu, Bahareh Sadeghi, and Edward W. Knightly. Enabling Vehicular Visible Light Communication Networks. In *Proceedings of the Eighth ACM International Workshop on Vehicular Inter-networking*, VANET, New York, NY, USA, 2011. ACM.

[7] F.J. Lopez-Martinez, G. Gomez, and J.M. Garrido-Balsells. Physical-Layer Security in Free-Space Optical Communications. *IEEE Photonics Journal*, 2015.

[8] A. Mostafa and L. Lampe. Physical-layer security for indoor visible light communications. In *IEEE International Conference on Communications*, 2014.

[9] A. Mostafa and L. Lampe. Securing visible light communications via friendly jamming. In *Globecom Workshops*, 2014.

[10] Gordon Povey. Top 10 Visible Light Communications Applications, 2011.

[11] Yijun Qiao, Harald Haas, and Edward Knightly. Demo: A Software-defined Visible Light Communications System with WARP. In *1st ACM Workshop on Visible Light Communication Systems*, 2014.

[12] Stefan Schmid, Josef Ziegler, Giorgio Corbellini, Thomas R. Gross, and Stefan Mangold. Using consumer led light bulbs for low-cost visible light communication systems. In *Proceedings of the 1st ACM MobiCom Workshop on Visible Light Communication Systems*, New York, NY, USA, 2014. ACM.

[13] Y. Y. Tan and W. Y. Chung. *Mobile health–monitoring system through visible light communication.* Bio-medical materials and engineering, 2014.

[14] A. Younis, W. Thompson, M. Di Renzo, C.-X. Wang, M.A. Beach, H. Haas, and P.M. Grant. Performance of spatial modulation using measured real-world channels. In *IEEE 78th Vehicular Technology Conference (VTC Fall)*, 2013.

[15] Bingsheng Zhang, Kui Ren, Guoliang Xing, Xinwen Fu, and Cong Wang. SBVLC: Secure barcode-based visible light communication for smartphones. In *Proceedings IEEE INFOCOM*, 2014.