Poster
Securing IoT through Coverage-Bounding Wireless Communication with Visible Light

Wang, Qing; Beysens, Jona; Singelee, Dave; Pollin, Sofie

DOI
10.1109/ICNP49622.2020.9259369

Publication date
2020

Document Version
Final published version

Published in
The 28th IEEE International Conference on Network Protocols, ICNP 2020

Citation (APA)
Wang, Q., Beysens, J., Singelee, D., & Pollin, S. (2020). Poster: Securing IoT through Coverage-Bounding Wireless Communication with Visible Light. In R. Guérin, & P. Steenkiste (Eds.), *The 28th IEEE International Conference on Network Protocols, ICNP 2020* IEEE. https://doi.org/10.1109/ICNP49622.2020.9259369

Poster: Securing IoT Through Coverage-Bounding Wireless Communication With Visible Light

Qing Wang†, Jona Beysens‡, Dave Singelée‡, and Sofie Pollin‡
†TU Delft, the Netherlands ‡KU Leuven, Belgium
Email: qing.wang@tudelft.nl {jona.beysens, dave.singelee, sofie.pollin}@kuleuven.be

***Abstract*—We propose a concept of coverage-bounding and *'visual'* wireless communication—HODOR[1]—to secure the Internet of Things (IoT). *Coverage-bounding* means the communication coverage is controlled accurately in 3-dimensions. *'Visual'* implies that the communication coverage and process are visible to user, representing an important and user-friendly side-channel for securing IoT. HODOR can provide secure wireless communication both *psychologically* (visible to users) and *technically* (nodes only communicate with each other within their delimited coverage). It can benefit IoT applications for secure wireless communications, especially those that demand secure interactions in proximity.**

I. Introduction

As the number of Internet of Things (IoT) devices increases rapidly, many efforts are being spent on preventing IoT threats. We propose HODOR, a coverage-bounding wireless communication system to secure IoT. The coverage-bounding is defined as: *the wireless communication range is controlled accurately in 3-dimensions.* As a result, potential IoT attacks would only occur in the delimited area. The main challenge in HODOR is how to bound the communication range accurately. To achieve that, we will exploit the directionality property of light and the emerging *Visible Light Communication (VLC)* technology.

Potential applications. Due to HODOR's properties of being visible and coverage-bounding, it can enhance the security of wireless communication both technically and psychologically. It can secure many IoT applications. For example, secure "watch-to-enter" access control (people open a door at several meters away from it by looking at the door-controller to send the necessary credentials; the door-controller can delimit its allowed access coverage; when exceeded, even people that have the correct credentials cannot open the door), convenient and secure payments in supermarkets (not needed to approach super close to "touch" a Reader for secure payment), and robot control in smart factories (robots are allowed to access certain resources through communications/interactions in proximity only if they are physically located in the delimited areas).

II. The Concept of HODOR

HODOR aims at enhancing the security of IoT applications. The key enabler is the bounded wireless communication range, delimited by nodes with accurate methods. It provides secure wireless communication both *psychologically* (users are aware of the communication process) and *technically* (nodes can only communicate with each other within their delimit coverage).

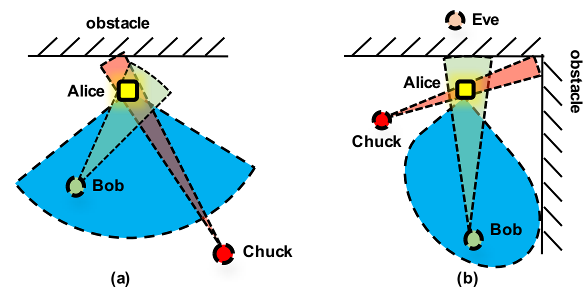

Fig. 1: Illustration of the proposed coverage-bounding wireless communications. Nodes can only talk with each other when in their delimited coverage. *Different shapes, e.g., sector, denote the coverage delimited by the corresponding nodes.*

Fig. 1 illustrates the proposed coverage-bounding and visual wireless communication, where nodes can only talk with each other when they physically stay in the delimited coverage. For example, in Fig. 1(a), Bob can talk with Alice; Chuck cannot because he is out of the communication coverage delimited by Alice[2]. Therefore, Alice can easily prevent the attacks from Chuck. Similarly, in Fig. 1(b), an attack/eavesdropping from Eve via non-line-of-sight links is physically prevented through Alice's delimited communication coverage via surrounding obstacles (e.g., walls). Besides, the communication medium is visible light. Therefore, Alice and Bob can observe where their data is transmitted. Thanks to this coverage-bounding wireless communication, potential attacks from the nodes that are out of the delimited coverage can be prevented. Consequently, attacks and even privacy leaks of the network could be reduced greatly.

III. Realizing HODOR

We propose two categories of preliminary methods to realize HODOR: *physical methods* and *software-defined methods*.

Physical methods. Here we exploit the physical properties of nodes and surroundings. Visible light is very directional. As a result, the direction of VLC signals is easy to control. For example, we can use a lens or an opaque tube to control the field-of-view of LEDs at the transmitters (TXs). Similarly, we can simply use an opaque tube at the photodiode of the receiver to only receive light from the delimited directions. Furthermore, visible light cannot penetrate opaque materials. Therefore, surrounding environment such as walls, cabinets, and curtain, can be leveraged to physically bound the wireless

[1] The name, derived from *hold the door*, is from the drama *Game of Thrones*.

[2] Even the signals sent by Chuck can reach Alice, if Alice detects that chunk is out of her delimited coverage, she will not decode the packets from Chuck.

978-1-7281-6992-7/20/$31.00 ©2020 IEEE

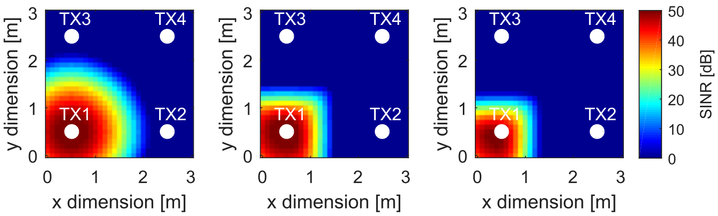

Fig. 2: Coverage-bounding by leveraging interference from neighbouring nodes. left) Only TX1 is used for communication; middle) TX2 and TX3 interfere with TX1 (have same transmission power); right) TX2 and TX3 interfere with 4x transmission power of TX1.

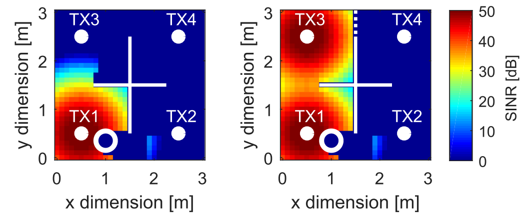

Fig. 3: Coverage-bounding by using blockages. The hollow circle denotes the human body; the white cross represents the cabinet; the dashed line represents curtain. left) Only TX1 is used; right) Both TX1 and TX3 are used.

communication area. Fig. 1(b) illustrates the use of walls to physically block VLC signals, preventing attacks from behind the wall. When needed, additional blockages can be added to surroundings to bound VLC signals. These methods are similar to isolated servers in which network interfaces are all blocked to prevent all the attacks from the Internet.

Software-defined methods. The second category of methods is software-defined, that can dynamically change the parameter settings of TXs, receivers, and even program the surroundings. LEDs, which are used to carry signals, are normally deployed densely in indoor areas. We could control several neighboring LEDs to transmit constructive/destructive VLC signals to delimit communication areas. If some LEDs modulate their light to interfere with surrounding VLC signals (i.e., in a destructive manner), we can shrink the communication coverage and even create specific shapes of the bounded communication area that can not be achieved with a single LED TX. Another software-defined method is to dynamically change the environment. In RF communication areas, programming the environment and channel through intelligent surface have been proposed very recently to improve the communication performance [1]. Recently, new materials have been developed that can dynamically change between opaque and transparent, e.g., chameleon-like smart glass [2]. These advanced materials could be controlled in software to change the delimited VLC coverage.

IV. Preliminary Evaluation

Simulation. We build a simulator in Matlab. We consider an area of $3\,\mathrm{m} \times 3\,\mathrm{m}$ consisting of a grid of 4 TXs. The TXs are aligned in an array with $2\,\mathrm{m}$ inter-TX distance and attached at a height of $2.8\,\mathrm{m}$ from the ground, facing downwards. Each TX is equipped with one LED. The half power semi angle of each LED is $15°$. The LED data is based on the off-the-shelf CREE XT-E LED [3], which is also used in our experiments. A receiver is placed on a desk with a perpendicular distance of $2\,\mathrm{m}$ from the TXs, facing upwards. The field of view of the photodiode at the receiver is $90°$.

Fig. 2 shows the simulation results by operating some TXs to send interfering signals. From Fig. 2(b) and (c), we observe that rectangle-shaped coverage-bounding is achieved. By adapting the transmission power of interfering TXs, different sizes of the bounded rectangle can be obtained. Fig. 3 shows the effect of blockages. We consider three blockages: (1) human body, modelled as a cylinder with 0.40 m diameter and 1.80 m height, and placed 0.35 m from TX1; (2) a cross-shaped cabinet with size $1.5\mathrm{m}\times 2\mathrm{m}\times 2\mathrm{m}$, placed in the middle;

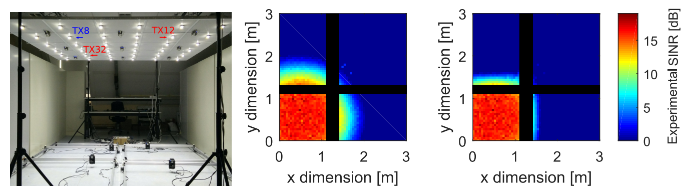

Fig. 4: Experimental validation in our DenseVLC testbed [4]: left) Setup; middle) Only TX8 is used; right) TX12 and TX32 interfere with TX8 (have same transmission power).

(3) curtain, with length of 0.5 m and height of 2 m, attached to the cabinet. From Fig. 3 we can see that by taking advantages of these surrounding environment that are common in our life, we can bound the communication coverage to different shapes and sizes. In the future when smart materials are used in our daily life [2], we could dynamically program our surroundings to bound, with more flexibility, the communication coverage required by different applications.

Experiment. We also experimentally evaluate HODOR. The experiments are performed with our DenseVLC [4]. The setup is similar to the one used for Fig. 2(b). We select three TXs from the 36 TXs in DenseVLC: TX8, TX12, and TX32, as indicated in Fig. 4(left). TX8 sends the desired signal to the receiver while TX12 and TX32 act as interfering nodes. We observe from Fig. 4(right) that in practice we do can bound the communication range as desired, e.g., to a rectangle, by leveraging neighboring nodes that transmit interfering signals.

V. Conclusion

We have presented in this paper our vision of HODOR, a visual and coverage-bounding wireless communication system designed specifically to secure proximity communications and interactions for the Internet of Things. In HODOR, attacks can only occur in bounded areas, which has the ability to significantly reduce potential attacks and privacy leaks. We envision that such a coverage-bounding wireless communication could open up a new line of research in IoT security and the general wireless communication areas.

References

[1] Z. Li and et al., “Towards programming the radio environment with large arrays of inexpensive antennas,” in *Proc. of USENIX NSDI*, 2019.
[2] Llordés and et al., “Tunable near-infrared and visible-light transmittance in nanocrystal-in-glass composites,” *Nature*, 2013.
[3] “CREE XT-E LED,” *https://goo.gl/ocs7bP*.
[4] J. Beysens and et al., “A cell-free networking system with visible light,” *IEEE/ACM Transactions on Networking*, 2020.