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).

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

978-1-7281-6992-7/20/$31.00

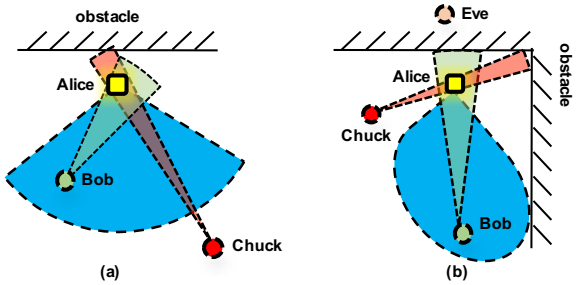

Fig. 1: Illustration of the proposed coverage-bounding wireless communications. Nodes can only talk with each other when in their delimited coverage. *Different shapes, e.g., sector, denote the coverage delimited by the corresponding nodes.*

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

[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.