HlcAuth: Key-free and Secure Communications via Home-Limited Channel

Chaohao Li[12], Xiaoyu Ji[12†], Xinyan Zhou[1], Juchuan Zhang[1]
Jing Tian[3], Yanmiao Zhang[1], Wenyuan Xu[1†]
[1]Zhejiang University
[2]Alibaba-Zhejiang University Joint Institute of Frontier Technologies
[3]University of South Carolina
Emails: {lchao, xji, xinyanzhou, juchuanzhang, yanmiaozhang, xuwenyuan}@zju.edu.cn, {tian9@email.sc.edu}

ABSTRACT

Nowadays most IoT devices in smart homes rely on radio frequency channels for communication, making them exposed to various attacks. Existing methods using encryption keys may be inapplicable on these resource-constrained devices that cannot afford the computationally expensive encryption operations. Thus, in this paper we design a key-free communication method for such devices. In particular, we introduce the Home-limited Channel (HLC) that can be accessed only within a house yet inaccessible for an outside-house attacker. Utilizing HLCs, we propose a challenge-response mechanism to authenticate the communications inside a house. The advantages of the `HlcAuth` protocol are low cost, lightweight as well as key-free, and requiring no human intervention. We show that `HlcAuth` can defeat replay attacks, message-forgery attacks, and man-in-the-middle (MiTM) attacks, among others. `HlcAuth` achieves 100% true positive rate (TPR) within 4.2m for in-house devices while 0% false positive rate (FPR) for outside attackers.

CCS CONCEPTS

• **Security and privacy → Security protocols**;

KEYWORDS

smart home, home-limited channel, challenge-response, key-free

ACM Reference Format:
Chaohao Li, Xiaoyu Ji, Xinyan Zhou, Juchuan Zhang, Jing Tian, Yanmiao Zhang, Wenyuan Xu. 2018. HlcAuth: Key-free and Secure Communications via Home-Limited Channel. In *ASIA CCS '18: 2018 ACM Asia Conference on Computer and Communications Security, June 4–8, 2018, Incheon, Republic of Korea.* ACM, New York, NY, USA, Article 4, 7 pages. https://doi.org/10.1145/3196494.3196499

1 INTRODUCTION

A typical smart home will include 500 smart devices by 2022 [14]. These smart devices have greatly improved the quality of people's daily life by allowing users to interact and control home appliances in both local and remote manners. However, the proliferation of IoT smart devices in smart homes induces security vulnerabilities and privacy concerns [3, 9, 11, 17]. By breaking the communication between these smart home devices, one can launch replay attacks, message-forgery attacks, and man-in-the-middle attacks from outside the home. In this paper, we propose a secure communication scheme to eliminate attacks from outside attackers.

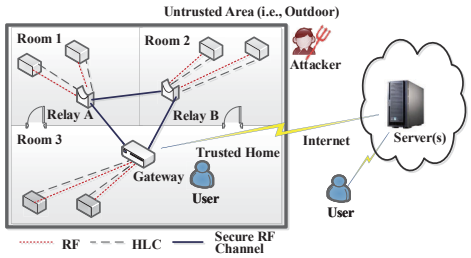

Figure 1: The architecture of a `HlcAuth` based smart home system.

In a typical smart home (shown in Fig. 1), smart devices and gateways form a home network, and they communicate via one of the standard wireless communication protocols, e.g., Zigbee, Z-Wave, WiFi and etc. When a user wants to control a device, he maneuvers the application. Then, the application sends the command to a server via the Internet, which in turn relays the command to the gateway. Finally, the gateway transmits the command to the target device in a wireless way. Although numerous secure communication protocols [5] can be applied to protect the communication between applications and gateways, the key challenge is **how to protect the wireless communication between the gateways and all smart devices, especially the devices that are resource-constrained**. This is the focus of this paper.

Traditional encryption-based methods may be computationally too expense for resource-constrained smart devices. For instance, validating an RSA-based signature may overwhelm a light bulb. Much effort has been devoted to designing a lightweight authentication scheme [8, 10]. Poor practices, such as choosing weak keys or sharing one key among all devices, are not unusual and result in vulnerabilities. To address the issue, we design a key-free communication strategy that does not rely on distributing cryptography keys and is applicable to all devices that have various degrees of computation capability.

The basis of our strategy is that it is the gateway that sends out control commands to smart devices, and gateways are typically

[†]Corresponding faculty authors.

ASIA CCS '18, June 4–8, 2018, Incheon, Republic of Korea

ACM ISBN 978-1-4503-5576-6/18/06…$15.00
https://doi.org/10.1145/3196494.3196499

located inside a home. We consider the inside area as a trusted environment, since the home area is physically isolated by walls and doors. As such, validating the authenticity of commands is equivalent to ensuring that the sender of the commands is located inside the trusted areas, e.g., a house or an apartment. Thus, we can avoid the complication imposed by key management and rely on the home-area physical property instead. To validate whether a sender is located inside a house, we study the *home-limited channels* (HLCs) and design a *HLC-based challenge-response* protocol (hereafter `HlcAuth`) for key-free and secure communication in smart homes. The key of HLC is that only when both the sender and a receiver are inside a home, can they reliably communicate. If either party is outside a home, they can no longer hear each other. To construct an HLC, we investigate a few communication medias, and choose three candidates—infrared, ultrasound and modulated visible light (MVL). All three candidates are imperceptible and boundary-attenuated.

Our proposed HLC-based command authentication scheme—`HlcAuth` works as follows. A gateway sends a control command to a device using the traditional wireless channel. To validate whether the command is indeed sent by the gateway, the device initiates a challenge-response query to the gateway. If the gateway passes the challenge-response test within an allowed window time, the device concludes that the command is valid. All messages that are associated with the challenge-responses are transmitted over HLC. The underlying principle is that no compromised device can be in the home area or no attacker can enter the home, only the gateway inside the home can receive the challenge and send a response over an HLC.

In summary. the contributions of our paper are listed as follows:

- We proposed the concept of home-limited channels and investigated candidate communication medias.
- We designed `HlcAuth`, a light-weight challenge-response protocol, for authenticating smart devices without using any cryptography key.
- We implemented and tested `HlcAuth` in four different physical scenarios. Results show `HlcAuth` can achieve 100% TPR within 4.2m and 0% FPR for devices in home .

2 BACKGROUND AND THREAT MODEL

In this section, we introduce the components of a typical smart home system and present our threat model.

2.1 Smart Home Architecture

As shown in Fig. 2, a modern smart home system generally consists of four parts: 1) smart devices, 2) gateway(s), 3) server(s), 4) one or several clients. Typically, smart devices communicate with a home gateway over RF channels using home area network (HAN) protocols (e.g. ZigBee, Wi-Fi), and the gateway communicates with a server and users' mobile devices over the Internet. The server is a trusted entity, and is responsible for long-term storage and analysis over large data streams. Users can operate smart devices through the home gateway directly or indirectly through an application.

The gateway takes responsibility for controlling the network data, devices and network interoperability. It can broadcast commands and queries to devices in the HAN, whenever needed. Smart

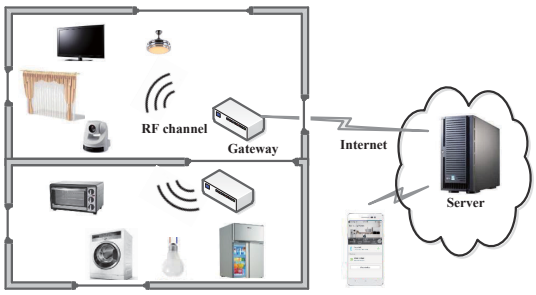

Figure 2: A typical smart home system.

devices transmit home data to the gateway using a single-hop link, and the communication between smart devices should be forwarded by the gateway. In addition, a smart home system may have multiple home gateways, which are distributed in the different rooms. They generally communicate with each other over secure RF channels with encryption.

2.2 Threat Model

The attacker's goal is to control smart devices and get user information by exploiting the vulnerabilities in home area networks. First, we assume prior work like "ZKP authentication" [5] are employed to protect the communication between gateways and applications, such that an attacker cannot inject forged messages to control smart devices by this link. Second, we assume that attackers cannot gain physical access to the smart home while they can launch various attacks over RF and HLC channels, and hereafter we call them local outside attackers. Here we describe the characteristics and abilities of local outside attackers in detail, as follows.

No Physical Access into a House. Since the smart home is an enclosed and private space, malicious attackers generally cannot gain physical access to the home. Numerous work and reports [3, 9, 11, 17] have shown that local attackers who are close to HAN yet outside the trusted home can hack into the HAN and control smart devices. Therefore, this paper focuses on defending against local outside attackers.

Multiple Attacks. Attackers may launch the following attacks over the RF and HLC channel. 1) Replay attacks, whereby an attacker records a valid command transmission and repeats it. 2) Man-in-the-middle (MiTM) attacks, whereby an attacker secretly relays and possibly alters the communication between the gateway and smart devices. 3) Message-Forgery attacks, whereby an attacker sends a fake command on behalf of a legal gateway.

Attacking Equipments. We assume that attackers can acquire both sensors (e.g. infrared and ultrasound sensors) and RF signal transceiver modules for eavesdropping, intercepting and injecting over RF and HLC channels.

3 HOME-LIMITED CHANNEL

In this section, we first define a home-limited channel (HLC) and further elaborate properties that required for it. Then we present three candidate HLCs—infrared, ultrasound and modulated visible light (MVL), and describe them in detail.

3.1 Definition and Properties

We define a *home-limited channel* as the channel of which the signal transmission range is within a home. For instance, signals transmitted over the indoor infrared channel can not be detected outside since infrared cannot penetrate the boundary (e.g., walls and doors) of a house. To achieve adequate security and usability, the following properties should be considered.

Boundary-attenuated means the signals over HLCs are intensely attenuated when propagating through the boundary of a residence, e.g., walls and doors. Thus, it is difficult for local outside attackers to launch replay, MiTM, or masquerade attacks.

Imperceptible. The message transmitted over HLC channels should be transparent to users, which means the transmission signals are supposed to be inaudible and unobservable.

Lightweight and Energy efficient. The data traffic over HLCs should be lightweight since numerous smart home devices are resource-constrained, and the transmission process over HLCs should be energy efficient. The extra-hardware of HLC sensors should be low-cost and easy to install.

3.2 HLC Candidates

According to the definition and properties of HLCs, we choose three HLC candidates—infrared, ultrasound and modulated visible light (MVL).

Infrared is a type of electromagnetic radiation that is invisible for users. The wavelength of common IR emitters is 940*nm*, which makes it reflected by walls and doors rather than penetrating them.

Ultrasound is sound waves with frequencies higher than the upper audible limit of human hearing. When ultrasound travels through the boundary of the smart home, its intensity diminishes with distance and the attenuation is generally proportional to the square of sound frequency.

Modulated Visible Light (MVL). we can modulate the pulse width of the visible light signals to make them below the human eye's resolution so that they are invisible for users.

4 DESIGN OF HLCAUTH PROTOCOL

Although the security properties of HLCs can efficiently prevent smart home from various attacks, it still leaves us two questions: 1) Since numerous smart devices are resource-constrained, how can we implement our scheme in a lightweight way? 2) Given that local outside attackers still have chances to eavesdrop or inject over HLCs, how can we further improve the security of communications? To answer above questions, we propose `HlcAuth`, which exploits a challenge-response mechanism and authenticates communications without keys. The overview of `HlcAuth` is shown in Fig. 3.

Challenge-Response. We utilize a challenge-response mechanism to realize the mutual authentication between the gateway and smart devices. Smart devices require the gateway to prove its trustworthiness by answering a correct *response*. Similarly, the gateway verifies the identity of smart devices by checking the validity of the *challenge*. Both *challenge* and *response* messages are transmitted over HLCs.

Key-free. The main difference between `HlcAuth` and traditional secure protocols is key-free, which means the authentication between smart devices and the gateway does not rely on encryption keys. The security of the communication relies on the boundary-attenuated property of HLCs.

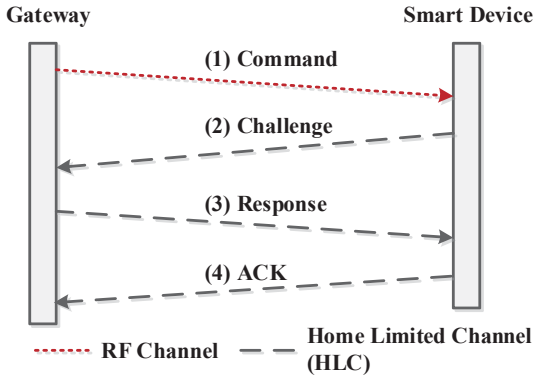

Figure 3: The overview of `HlcAuth`. The *command* message is transmitted over the RF channel while the *challenge, response* and *ACK* message is transmitted over the HLC.

4.1 Protocol Design

Here we describe the detailed protocol of `HlcAuth` and summarize notations in Table. 1. `HlcAuth` includes four phases: RF command initiation, HLC challenge, HLC response and command execution.

4.1.1 ***Phase I: Command (RF).*** *HG* performs the following steps to initiate a standard RF *command*, which is transmitted using the existing HAN protocol (e.g. Zigbee, Z-Wave), to *SD*s.

S1. *HG* first generates a unique short authentication token $Token_{cm}$ and then records its current local timestamp T_{g1}. Both are used to prevent replay attacks.

S2. *HG* sends the *command* message, which includes the $P_{cm} = \{ID_a \,||\, ID_g \,||\, Seq_{cm} \,||\, CMD \,||\, Token_{cm} \,||\, CRC_{cm}\}$ to Device *A* over RF channels.

S3. *HG* computes $Q_{cm} = h(ID_a \,||\, Seq_{cm} \,||\, CMD \,||\, Token_{cm})$ and stores the $(Seq_{cm}, Token_{cm}, Q_{cm})$ into its cache.

4.1.2 ***Phase II: Challenge (HLC).*** Upon receiving the *command* message from *HG*, device *A* sends a *challenge* message to authenticate *HG*.

S4. Device *A* generates a unique short random authentication token $Token_{cl}$ and computes $Q_{cm'} = h(ID_a \,||\, Seq_{cm} \,||\, CMD \,||\, Token_{cm})$. At the same time, it records its current local timestamp T_{d1}.

S5. Device *A* sends a *challenge* message $P_{cl} = \{ID_a \,||\, ID_g \,||\, Seq_{cl} \,||\, Q_{cm'} \,||\, Token_{cl} \,||\, CRC_{cl}\}$ to *HG* over HLCs.

S6. Device *A* computes the hash value $Q_{cl} = h(ID_g \,||\, Seq_{cl} \,||\, Q_{cm'} \,||\, Token_{cl})$ and stores the $(Seq_{cl}, Token_{cl}, Q_{cl})$.

4.1.3 ***Phase III: Response (HLC).*** After receiving the *challenge* message from the device *A*, *HG* first verifies the integrity of the *command* message and then sends the *response* message to device *A* over HLCs.

S7. Upon receiving the *challenge* message from device *A*, *HG* records its current local timestamp T_{g2} and checks whether $(T_{g2} - T_{g1}) \leq \Delta T$. If it holds then *HG* retrieves the corresponding Q_{cm} from its cache, else sets $Q_{cl'}$ to zero.

S8. *HG* verifies whether $Q_{cm'} = Q_{cm}$. If not, *HG* sets $Q_{cl'}$ to zero, else it computes the $Q_{cl'} = h(ID_g \,||\, Seq_{cl} \,||\, Q_{cm'} \,||\, Token_{cl})$.

S9. *HG* sends a *response* message $P_{rs} = \{ID_a \,||\, ID_g \,||\, Q_{cl'} \,||\, CRC_{rs}\}$ to device A over HLCs.

4.1.4 ***Phase IV: Execution (HLC).*** In this phase, device *A* verifies the locality of *HG* and the integrity of the *challenge* message. If the *response* message passes the verification, the device *A* executes the *command* and returns an ACK message, which includes its status to *HG* over HLCs .

S10. Upon receiving the *respond* message from *HG*, device A records its current local timestamp T_{d2} and checks whether $(T_{d2} - T_{d1}) \leq \Delta\, T$. If it holds then device A retrieves the corresponding Q_{cl} from own cache, else aborts the process.

S11. Device A verifies whether $Q_{cl'} = Q_{cl}$, if yes then it executes the *command*, else aborts the process.

S12. Device A returns an ACK message $P_{ack} = \{ID_a \,||\, ID_g \,||\, DS_a \,||\, CRC_{ack}\}$ to *HG* over HLCs.

4.2 Packet Transmission Scheme

Here we elaborate the packet transmission scheme of `HlcAuth`, which includes frame design and modulation scheme of three HLC candidates.

The goal of the frame design is to minimize the overhead while ensuring the integrity of the message. The detailed frame design of the *challenge*, *response* and *ack* message is summarized in Table 2, Table 3 and Table 4, respectively.

Each *challenge* frame contains the following information: ID_a, ID_g, Seq_{cl}, $Q_{cm'}$, $Token_{cl}$ and CRC_{cl}. In our scheme, we utilize the MD5 algorithm to calculate the hash value, and use a half of the hash result (64 bits) to reduce the size of the payload. Since the computation complexity of the MD5 is $O(n)$ and the length of each frame is no more than 150 bits, we can properly apply MD5 on resource-constrained devices.

For the *response* and *ack* frames, we remove the identity of the frame and secure token to further reduce the overhead. The hash function applied in the *response* and *ack* frames is the same as the *challenge*'s. Since the length of the *ack* frame is limited, we use CRC-4 rather than CRC-8.

In `HlcAuth`, we utilize the NEC IR modulation scheme [1] for infrared, Pulse Position Modulation (PPM) [7] for modulated visible light (MVL) and Binary Frequency-shift keying (BFSK) [18] for ultrasound, respectively.

5 SECURITY ANALYSIS

In this section, we analyze the security of `HlcAuth` against various types of attacks, including replay, message-forgery and man-in-the-middle (MiTM) attacks.

5.1 Replay Attack

A local outside attacker can intercept the RF *command* packet and further repeat it without modification. However, each valid *command* with a unique $Token_{cm}$ and Seq_{cm} has time effectiveness. In the phase of RF command initiation, the home gateway will store the $(Seq_{cm}, Token_{cm}, Q_{cm})$ into its cache, and retrieve them until receiving the *challenge* packet. After verifying the validation of the *challenge*, home gateway will remove the $(Seq_{cm}, Token_{cm}, Q_{cm})$ locally. Therefore, the replayed *command* packet cannot pass the verification since there is no corresponding $(Seq_{cm}, Token_{cm}, Q_{cm})$ in the home gateway's cache.

5.2 Message-Forgery Attack

Assume that a local outside attacker can capture previous legal *command* messages and obtain all possible combinations of the (ID_a, ID_g, CMD). Thus, she can forge an arbitrary RF *command*.

According to the challenge-response mechanism, a potential message-forgery attack requires the following two steps: *i*) forge an RF *command*; *ii*) forge an HLC *response*. After sending the fake *command* packet, the attacker will face the following situations.

(1) When device *A* receives a forged *command* packet, it will initiate an HLC *challenge* to the home gateway. Since this *challenge* packet is built on the forged *command*, it will generate a fake $Q_{cm'}$ which cannot be consistent with any Q_{cm} stored in the home gateway's cache. Thus, the *challenge* message cannot pass the verification.

(2) One possible way for the attacker to avoid the failure of the *challenge* check is sending a forged HLC *response* before the home gateway returns the termination signals. To address this issue, `HlcAuth` sets two barriers to defend against such attacks. First, both eavesdropping and transmitting are over HLCs, thus local outside attackers have extremely low probability to successfully implement attacks. Second, the time for completely sending a forged *response* packet is limited. According to our later experiments, the duration of sending a *response* packet over HLCs is more than $300ms$ while the interval between legal *challenge* and *response* packet is $27ms$. That means the attacker can not send a forged *response* packet integrally.

5.3 MiTM Attack

We consider MiTM attackers with two types of goals: 1) modify the ID_a of a *command*; 2) modify the *CMD* of a *command*. Since we assume RF channels are available to attackers, thus it is feasible for them to modify (ID_a, CMD, CRC_{cm}) in RF packets. To further implement MiTM attacks, the attacker needs five steps: 1) intercept the valid *challenge* packet; 2) eavesdrop the valid *challenge* packet; 3) send a forged *challenge* packet; 4) intercept the valid *response* packet; 5) send a forged *response* packet. In this process, the attacker will face the following challenges:

First of all, it is hard for attackers to find out when the *challenge* packet begins to transmit, since the attacker has extremely low probability to successfully eavesdrop HLCs. Once he misses the start point of the packet, he can't get the unique $(Seq_{cl}, Token_{cl})$ correctly. Even if the attacker can get the start point, it is still difficult for him to get the integrated information due to the boundary-attenuated property of HLCs. Compared to the message-forgery attack, MiTM attacks need one more HLC transmission, which will further decrease their success rate.

6 EVALUATION

In this section, we evaluate the performance of `HlcAuth` from the aspects of usability and security.

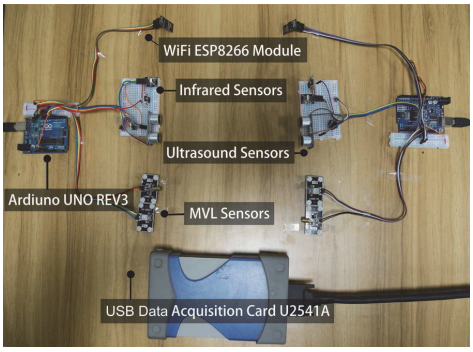

Figure 4: Experiment setup.

6.1 Experiment Setup

We build gateways and smart devices using Arduino UNO REV3 Development Boards with ESP8266 WiFi module. Each device is equipped with a 940nm SOURCEKIT infrared emitter, an HX1838B infrared receiver, a KY-008 650nm red MVL transmitter, a GY-485-44009 RS485 light intensity sensor, and an HC-SR04 ultrasound transducer. To guarantee the HLC signals can cover the whole room, the gateway is equipped with two sets of HLC sensors on its both sides. We also deploy our prototype in a $3m * 2.5m * 3m$ room. The experiment setup is shown in Fig. 4.

We assume that attackers can locate at any position outside the house. We select four positions in the experiments: an attacker stays behind 1) a 6cm thick metal door, 2) a 30cm wall, 3) a 3cm covered window, and 4) a 3cm glass window, respectively.

Evaluation Metrics. To quantify usability, true positive rate (TPR) is used. TP denotes the number of legal *commands* that are correctly executed, while FN represents the number of *commands* that the device doesn't execute as expected. We utilize false positive rate (FPR) to quantify security. FP denotes the number of the forged *commands* from the attacker that are executed, while TN denotes the number of forged commands being rejected successfully.

$$TPR = \frac{TP}{TP + FN}, \quad FPR = \frac{FP}{FP + TN} \tag{1}$$

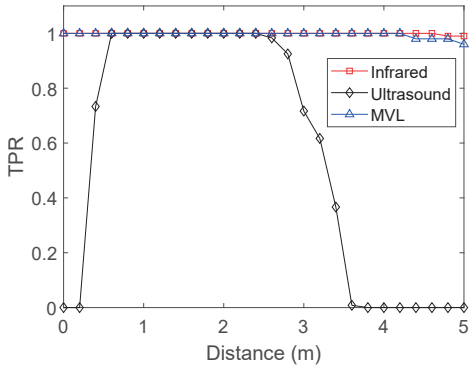

Figure 5: The TPR of infrared, ultrasound, and MVL-based HLC at various distances. Both infrared and MVL can achieve a TPR of 100% within 4.2m and 96% at 5m while ultrasound can only achieve a TPR of 100% between 0.6m to 2.6m.

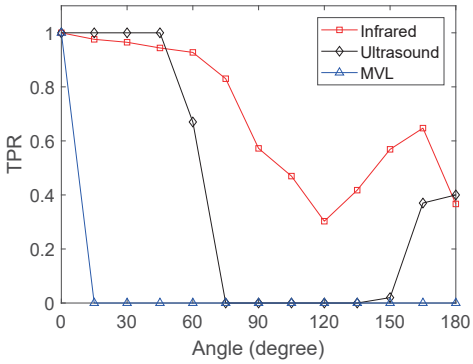

Figure 6: The TPR of infrared, ultrasound, and MVL-based HLC at various angles at 2m. Both infrared and ultrasound can achieve over a TPR of 94% within 45°.

6.2 Usability

To measure the usability of `HlcAuth`, we evaluate the performance of HLC candidates from the aspects of distances and angles.

Distance: We measure the TPR of infrared, ultrasound and MVL by varying the distances from 0m to 5m. The device and the gateway are placed facing each other, i.e., the angle of the device and the gateway is 0. We test the TPR once every 20cm, and we send the command 50 times at each point. The results are shown in Fig.5. Both infrared and MVL can achieve 100% TPR within 4.2m, and will degrade slightly at a further distance. It is worth mentioning that the TPR of infrared and MVL is 98% and 96% respectively, even when the distance reaches 5m. However, ultrasound can only achieve 100% TPR at a distance between 0.6m and 2.4m, and the TPR will decline to 0 out of this range. The ultrasound cannot success in such a short distance because it is modulated by FSK. The signal is distorted and cannot be demodulated at a further distance. Considering the application scenarios (e.g., a large living room), the range of ultrasound is insufficient to guarantee a high TPR. Thus, we cannot use an ultrasound to transmit HLC.

Angle: Given that the transceiver of the device and the gateway is not always facing each other, we evaluate the impact of angles on the TPR. We test the performance of three candidates by placing the device and the gateway at an angle from 0° to 180° at 2m at an interval of 15°, and each HLC is tested 50 times at each point. The results are presented in Fig.6. Both infrared and ultrasound can achieve relatively high TPR within 45°, while MVL can only communicate at 0° because of its high directionality. As the angle increases, the TPR of ultrasound decreases to 0 at 75° while the TPR of infrared decreases slower and reaches the minimum (30%) at 120°. Interestingly, when the angle is approaching 180°, there is a small rise as a result of the reflection of wall.

In conclusion, infrared is the best HLC candidate due to its relative high TPR at a long distance and a large range of angle, while ultrasound and MVL are both deficient due to attenuation or high directionality.

6.3 Security

We further validate the security of `HlcAuth` experimentally from the perspective of FPR and time limitation.

We let a malicious gateway to mimic a local outside attacker who tries to stay as close as possible to the smart home. Then we move the indoor victim from $0m$ to $3m$ away from the boundary at a $10cm$ step and calculate FPR.

The results show that the FPR is 0 when using infrared, ultrasound or MVL signals to build `HlcAuth`. Thus, attackers cannot successfully send or receive packets reliably when locating outside the boundary of the smart home. Although the high-power infrared and MVL signals can have small chance to penetrate glass window, attackers still fail to conduct various attacks due to the constrained timing. The constrained timing means that when the attacker have received the *challenge* message, she must finish the transmission of the entire *response* message before the user's gateway begins to send the legal *response* message. Since the infrared receiver cannot demodulate successfully when two infrared messages collide, the attack fails. Tests show that the transmission duration of a *response* message is around $325ms$ to $350ms$, which is much longer than the $27ms$ processing time of the *challenge* message.

ACKNOWLEDGMENTS

We would like to thank our shepherd Liqun Chen for her valuable contributions. This work is supported by NSFC 61472358, NSFC 61702451, and the Fundamental Research Funds for the Central Universities 2017QNA4017.

7 RELATED WORK

Smart Home Security. Current smart home security focus on smart devices and communication protocols. First, Denning *et al.* outlined a set of emergent threats to smart homes due to the vulnerability of the smart devices [2]. Notra *et al.* [15] dissect the behavior of three household devices, and the results show that these devices can be compromised. The communication protocols applied in the smart home was also found insecure. Molina [13] utilized the KNX package flaws to realize the remote control on a HA system.

To improve the security of the communication in smart home systems, existing work focuses on building up a lightweight authentication scheme between smart home devices. Kumar *et al.* [8] used a short authentication token and established a secure session key to reduce the cost of the public key operations. However, the system setup in this scheme requires a third-party service provider involvement, and the secure information that used to produce a session key has to be stored in home devices in advance. Li *et al.* [10] proposed that each node get private/public key pair from a certificate agent(CA) over an OOB channel and then carry out an authenticated key exchange protocol. However, this work does not include the implementation and no security analysis on OOB data distribution provided. Different from the above schemes, we propose a secure lightweight communication protocol based on home-limited channel with minimal additional cost.

OOB Channel. Typically, Out-of-band (OOB) Channels are used for device pairing [4, 12, 16] at bootstrap phase. According to the physical channel that signals communicate over, OOB channels can be categorized into acoustic [4], light [16], seismic, magnetic, thermal, and movement [12]. Traditional device pairing methods based on OOB channels are generally considered as secure. However, Halevi *et al.* [6] demonstrate the feasibility of eavesdropping acoustic OOB channels, which should be taken into account in our protocol design. In this paper, we utilize the home limitation of OOB channels to establish a secure communication protocol against local outside attacks from both RF and OOB channels.

8 CONCLUSION

We studied Home-Limited Channel (HLC) that can enhance the security of existing smart home– `HlcAuth`. Based on the boundary-attenuated property of HLCs, `HlcAuth` utilized challenge-response mechanism to realize the mutual authentication between the gateway and smart devices without key management. The security analysis revealed that the `HlcAuth` can defend against replay attacks, message-forgery attacks, and man-in-the-middle (MiTM) attacks. Our validation showed that `HlcAuth` can satisfy the usability (e.g., 100% TPR within $4.2m$, low time and energy consumption, and low cost) for the in-home devices while being resilient against various attacks conducted by local outside attackers. As a direction for future work, it is worth studying the impact of house boundaries, e.g., the thickness and materials of the walls.

REFERENCES

[1] Altium. 2017. NEC infrared Transmission Protocol. (September 2017). http://techdocs.altium.com/display/FPGA/NEC+Infrared+Transmission+Protocol.
[2] Tamara Denning, Tadayoshi Kohno, and Henry M. Levy. 2013. *Computer security and the modern home.* ACM. 94–103 pages.
[3] Behrang Fouladi and Sahand Ghanoun. 2013. Security evaluation of the Z-Wave wireless protocol. *Black Hat* (2013).
[4] Michael T. Goodrich, Michael Sirivianos, John Solis, Gene Tsudik, and Ersin Uzun. 2006. Loud and Clear: Human-Verifiable Authentication Based on Audio. In *IEEE International Conference on Distributed Computing Systems.* 10–10.
[5] Slawomir Grzonkowski and Peter M Corcoran. 2011. Sharing cloud services: user authentication for social enhancement of home networking. *IEEE Transactions on Consumer Electronics* 57, 3 (2011).
[6] Tzipora Halevi and Nitesh Saxena. 2013. Acoustic eavesdropping attacks on constrained wireless device pairing. *IEEE Transactions on Information Forensics and Security* 8, 3 (2013), 563–577.
[7] Jon Hamkins. 2007. Pulse position modulation. *Handbook of Computer Networks: Key Concepts, Data Transmission, and Digital and Optical Networks, Volume 1* (2007), 492–508.
[8] Pardeep Kumar, Andrei Gurtov, Jari Iinatti, Mika Ylianttila, and Mangal Sain. 2016. Lightweight and secure session-key establishment scheme in smart home environments. *IEEE Sensors Journal* 16, 1 (2016), 254–264.
[9] Andrew Laughlin. 2017. Could your smart home be hacked? https://www.which.co.uk/news/2017/06/could-your-smart-home-be-hacked/. (2017).
[10] Yue Li. 2013. Design of a Key Establishment Protocol for Smart Home Energy Management System. In *Fifth International Conference on Computational Intelligence, Communication Systems and Networks.* 88–93.
[11] Zhen Ling, Junzhou Luo, Yiling Xu, Chao Gao, Kui Wu, and Xinwen Fu. 2017. Security Vulnerabilities of Internet of Things: A Case Study of the Smart Plug System. *IEEE Internet of Things Journal* PP, 99 (2017), 1–1.
[12] R. Mayrhofer and H. Gellersen. 2009. Shake Well Before Use: Intuitive and Secure Pairing of Mobile Devices. *IEEE Transactions on Mobile Computing* 8, 6 (2009), 792–806.
[13] Jesus Molina. 2014. Learn how to control every room at a luxury hotel remotely: The dangers of insecure home automation deployment. *Black Hat USA* 2014 (2014).
[14] Icontrol Networks. 2015. 2015 State of the Smart Home Report. https://www.slideshare.net/iangertler/2015-state-of-the. (2015).
[15] Sukhvir Notra, Muhammad Siddiqi, Hassan Habibi Gharakheili, Vijay Sivaraman, and Roksana Boreli. 2014. An experimental study of security and privacy risks with emerging household appliances. In *Communications and Network Security (CNS), 2014 IEEE Conference on.* IEEE, 79–84.
[16] N Saxena, J. E Ekberg, K Kostiainen, and N Asokan. 2006. Secure device pairing based on a visual channel. In *Security and Privacy, 2006 IEEE Symposium on.* 6 pp.–313.
[17] Symantec. 2015. Insecurity in the Internet of Things. (March 2015). https://pdfs.semanticscholar.org/6d7f/60b16adead96aafa9e975207980eb32671b5.pdf.
[18] Bob Watson. 1980. FSK: signals and demodulation. *Watkins–Johnson Company Tech–notes* 7, 5 (1980).

APPENDIX

A NOTATION

Symbol	Desciption
HLC	Home-limited channel
HG	Home gateway
SD	Smart device
ID_g	Identity of the home gateway
ID_a	Identity of smart device A
Seq_{cm}	The sequence number of each *command*
Seq_{cl}	The sequence number of each *challenge*
$Token_{cm}$	A unique authentication token for each *command*
$Token_{cl}$	A unique authentication token for each *challenge*
CMD	The command to operate devices
$h()$	One-way hash function
P_m	The package of the message
T_{gn}	The n^{th} timestamp of the home gateway
T_{dn}	The n^{th} timestamp of smart device A
CRC_m	Cyclic redundancy check of the message
DS_a	The status of smart device A
$\|\|$	Concatenation operation

Table 1: Notations

B FRAME STRUCTURE

Segment	ID_a	ID_g	Seq_{cl}	$Q_{cm'}$	$Token_{cl}$	CRC_{cl}
Length	8 bits	4 bits	8 bits	64 bits	8 bits	8 bits

Table 2: HLC Challenge Frame

Segment	ID_a	ID_g	$Q_{cl'}$	CRC_{rs}
Length	8 bits	4 bits	64 bits	8 bits

Table 3: HLC Response Frame

Segment	ID_a	ID_g	DS_a	CRC_{ack}
Length	8 bits	4 bits	8 bits	4 bits

Table 4: HLC ACK Frame