OptiSec3D - A new Paradigm in Secure Communication and Authentication featuring Time-of-Flight

Hannes Plank* Matthias Almer† Robert Lobnik* Christian Steger†
Thomas Ruprechter* Holger Bock* Josef Haid* Gerald Holweg* Norbert Druml*
*Infineon Technologies Austria AG, Design Center Graz
†Graz University of Technology, Institute for Technical Informatics
{hannes.plank, robert.lobnik, thomas.ruprechter, holger.bock, josef.haid,
gerald.holweg, norbert.druml}@infineon.com
matthias.almer@student.tugraz.at steger@tugraz.at

Abstract

Information security and trust represent fundamental requirements for today's information and communication systems as well as interconnected embedded systems. If these requirements are not tackled properly, security attacks, such as relay attacks, may compromise these systems severely.

Here we introduce OptiSec3D, a new paradigm in secure communication systems. The presented approach for secure communication and authentication uniquely enhances the key enabling Time-of-Flight 3D localization technology with optical communication abilities. By extending these features with state-of-the-art security anchors, new levels of trust and security can be reached for information and communication systems.

This work not only provides the background and concept of this secure communication and authentication approach, but also demonstrates its feasible implementation by means of a very first prototype. Furthermore, we outline how security attacks, such as relay attacks, can be counteracted and how future OptiSec3D-based security-critical systems will look like.

Keywords

Information Security, Optical Communication, Contactless Authentication, Time-of-Flight, 3D Localization

1 Introduction

Today, trust and information security is one of the key requirements for embedded systems that are interconnected through wired or wireless communication technologies. If such embedded systems are not designed properly, security breaches may have far-reaching consequences. For example, passive keyless entry and start systems, which are widely used in the automotive domain and deemed secure in the past, have been compromised because of missing distance checks (i.e., evaluation of whether the transponder is in the range of the reader or not). This example, cf. [5], demonstrates that in order to provide secure embedded communication systems, further parameters (such as distance and localization information of communication partners) are essential for proper trust establishment.

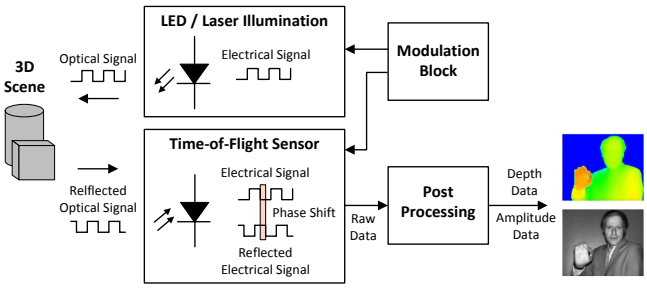

Figure 1. Working principle of PMD-based Time-of-Flight 3D sensing. Obtained with changes from [3].

This paper tackles this gap and proposes an innovative solution for secure communication systems, which is based on the key enabling Time-of-Flight technology and state-of-the-art security anchors (such as Infineon's security controllers). Time-of-Flight is a depth sensing method that provides distance information by measuring the travel time of emitted light. There are direct and indirect Time-of-Flight measurement approaches, cf. [14]. This work focuses on the indirect method, which calculates depth distance information by evaluating the phase shift of an emitted infrared light with the help of photonic mixing devices (PMD), cf. [10]. Figure 1 depicts the basic working principle of a PMD-based camera system. In theory, since the emitted infrared light is modulated, data can also be exchanged between two Time-of-Flight imaging systems.

We propose a new secure communication interface through uniquely extending the Time-of-Flight technology's 3D environment sensing with optical communication capa-

International Conference on Embedded Wireless Systems and Networks (EWSN) 2016
15–17 February, Graz, Austria

ISBN: 978-0-9949886-0-7

bilities and state-of-the-art security anchors. The 3D information gathered by the camera can then be used to verify, e.g., localization information (e.g., both communication partners check if they both measure the same distance) or the communication partner's 3D geometry.

Summarizing, this paper makes the following contributions:

- It introduces OptiSec3D, a new approach for secure communication systems featuring Time-of-Flight depth sensing.
- It outlines how today's information security challenges can be tackled with help of OptiSec3D.
- It demonstrates that the presented concept can be feasibly implemented by means of a very first prototype.

This paper is structured as follows. Section II gives a short introduction into the related work covering the topics of related communication techniques. Furthermore, it discusses today's security challenges in contactless communication. In Section III, our novel security concept based on Time-of-Flight is presented. Followed by Section IV which demonstrates our very first OptiSec3D system prototype. Finally, our results are concluded and some details about our future work are given in Section V.

2 Related Work

2.1 Communication Technologies

Given the fact that Time-of-Flight 3D sensing systems use an active and modulated illumination source (such as an LED or a laser operating in the infrared spectrum, which is depicted in Figure 1), data can be exchanged between two systems. Yuan et al. [16] demonstrated with an early prototype that data transfer between a modulated light source and a Time-of-Flight sensor is possible. The authors developed an LED array, which is able to transfer information to a Time-of-Flight camera. The communication in this system is however one-way only. The LED array system senses the modulation frequency and repeats the signal with information modulated into the phase shift. There is no information sent from the Time-of-Flight camera and furthermore this approach does not deal with security aspects at all.

Another well-known interface technology that relates to the introduced secure communication concept is Near Field Communication (NFC). Today, NFC is used in our everyday life, e.g., in the fields of transportation, payment, loyalty and coupons, logistics, healthcare, and access control (cf. [4]). Given these application fields, the security of an NFC-based reader / transponder system is of high importance; as summarized by the authors in [8] and [7]. In order to make security attacks more difficult, standardized security methods are employed, such as elliptic-curve cryptography. Furthermore, the distance between reader and transponder is limited to a maximum of 10cm: the reader emits an alternating magnetic field, which is used to power the transponder and to exchange data with it. Therefore, by limiting the reader's output power, the range of operation is limited as well. However, a maliciously modified reader, which emits a very strong magnetic field, enables communication over a distance of meters.

In the field of optical communication systems, famous

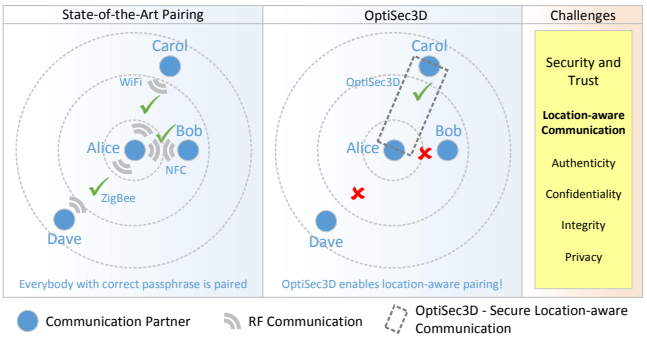

Figure 2. Comparison between state-of-the-art pairing, the OptiSec3D approach, and the challenges ICT systems are confronted with.

and simple solutions are the Consumer IR and IrDA technologies. While Consumer IR is used to control consumer electronics over distances of some meters, IrDA was designed for short range only. A novel technology in the field of optical data communication is Li-Fi, which was used in 2014 in the first commercial product (cf. [13]). Li-Fi works in the visible light spectrum, uses LEDs, and achieves data rates that can compete with RF-based communication, such as WiFi. Harald Haas, the inventor of Li-Fi, predicts that in 25 years Li-Fi technology will be present in every light bulb and thus will lead to the Internet-of-Things, which connects every electronic device to the Internet.

2.2 Challenges in Today's Contactless Authentication Solutions

Providing security and trust represents a fundamental requirement for today's information and communication systems. Ravi et al. outline in [12] the challenges that are faced when designing and developing secure embedded systems. As illustrated in Figure 2, the missing awareness for location and distance is one of the key challenges for today's information and communication technology systems (such as NFC, WiFi, ZigBee). For instance, WiFi- or Bluetooth-based pairing procedures accept all communication partners that provide the correct pass-phrases, regardless of distance or location verifications. This missing verification enables a set of malicious attack vectors.

Several authentication and identification systems, although deemed secure in the past were compromised and spoofed successfully. As an example for a compromised type of authentication system, Francillon et al. showed in [5] that passive keyless entry and start systems, which are widely used in modern cars, can be hacked easily and with only little effort. The authors performed relay attacks on ten cars of eight manufacturers and were able to maliciously unlock, start, and drive these cars in each case. This incident reveals the need for further security measures, in particular location awareness, at system-level. If these keyless entry and start systems implemented proper verification of distance between car and key, such relay attacks would not be successful.

In passive and contactlessly powered RFID and Near Field Communication-based systems, the communication

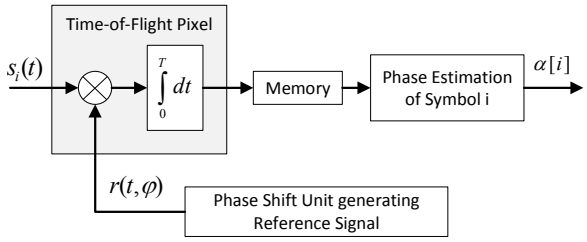

Figure 3. Physical principles of Time-of-Flight-based optical data transmission.

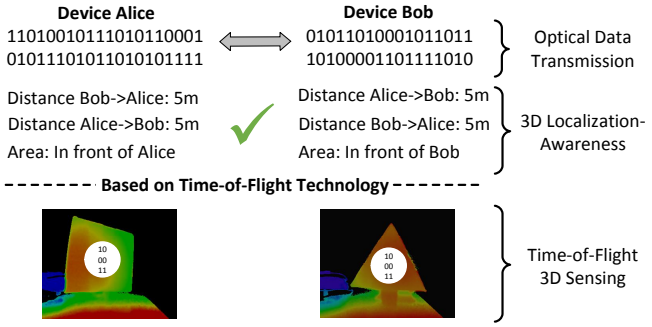

Figure 4. OptiSec3D exploits optical data transfer and 3D localization based on Time-of-Flight.

distance is restricted (typically to a maximum of 10 cm) by the technology. Thus, it is restricted by the strength of the magnetic field, which is emitted by the reader. Again, this poses an issue for the passive transponder, because it is hardly capable to verify the distance to the reader: for example, a maliciously modified reader emitting a very strong magnetic field can enable communication over a distance of meters, which makes a whole set of attacks possible.

In order to make such contactless and RF-based communication more secure, for example, the authors of [1] proposed a distance bounding protocol. This type of protocol estimates the round trip time of radio signals and thus can estimate the distance of the communication partners and can identify whether, e.g., a relay attack takes place. Hancke et al. showed in [6] that distance bounding protocols can also be feasibly implemented for RFID- and NFC-based communication systems. However, in [2], the authors demonstrated that even such sophisticated protocols are not 100% secure against cleverly designed attacks.

As another example, in [11], Prabhakar et al. presented a survey summarizing security issues in today's biometric-based authentication systems. The usage of cameras that are only capable to gather two-dimensional biometric information is one of the identified root causes for these so far unsolved security challenges. For instance, a photo or video can be employed for spoofing face recognition systems. Recently, Krissler demonstrated in [9] the vulnerability of today's fingerprint-based authentication systems: with the help of a fingerprint, which was recreated from high resolution pictures of Germany's Defense Minster taken during a public event, he was able to successfully spoof the biometric system. If biometric-based authentication systems employed 3D camera systems and communication between authentication partners, such spoofing attacks would not be successful at all. These examples support the view that fundamental challenges exist in several information and communication technology systems used today which makes them vulnerable to attacks:

- Communication-based systems usually do not verify distance or area information of their communication partners.
- Vision-based authentication systems usually do not support communication between authentication partners.

Summarized, in order to provide secure authentication and communication for critical fields of applications, it is essential to verify additional parameters (such as distance and localization information of communication partners). Although there is research in this field, there is a major gap in literature concerning the outlined challenges, which is addressed in our work.

3 OptiSec3D

3.1 Physical Principles

The principle of Time-of-Flight based communication works by phase modulation of the emitted infrared light. Figure 3 shows the principle of a pixel capturing the transferred symbol i. Time-of-Flight cameras are designed to measure phase differences between a reference signal $r(t,\phi)$ and incoming light $s_i(t)$. The incoming signal pulses are integrated for the integration time t. A shorter integration time means a higher frame-rate. The phase difference is converted to a voltage by a photonic mixture device, cf. [15], and is then digitized. The difference to the normal depth sensing purpose of Time-of-Flight systems is that the incoming light is sent directly from the communication partner, and the signal amplitude is relatively high. This allows to dramatically shortening the integration time and thus increasing the communication bandwidth. Since lots of pixels sense the optical signal at the same time, phase noise can be limited by averaging the measured phase. Using longer integration times for sensing the communication partner, and using short integration times for communication can be alternated multiple times per second. Furthermore, Time-of-Flight communication is based on modulated infrared light, which ensures high robustness against environmental influences, such as other light-sources.

3.2 Concept and Key Features

As highlighted in Figure 4, OptiSec3D will introduce a radically new communication technology. This is achieved by uniquely extending the key enabling Time-of-Flight 3D sensing technology with optical data communication (while using the same Time-of-Flight hardware) and with state-of-the-art security anchors. Today, there is no solution similar to OptiSec3D. The following key features will be enabled:

- Optical communication in conjunction with 3D location-awareness (e.g., 3D distance and area checks) will make communication-based and authentication-based applications (e.g., secure pairing of devices, payment) more secure and will reduce the probability for malicious attacks.

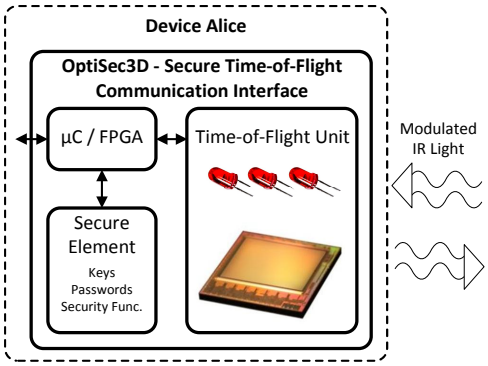

Figure 5. Proposed OptiSec3D communication interface.

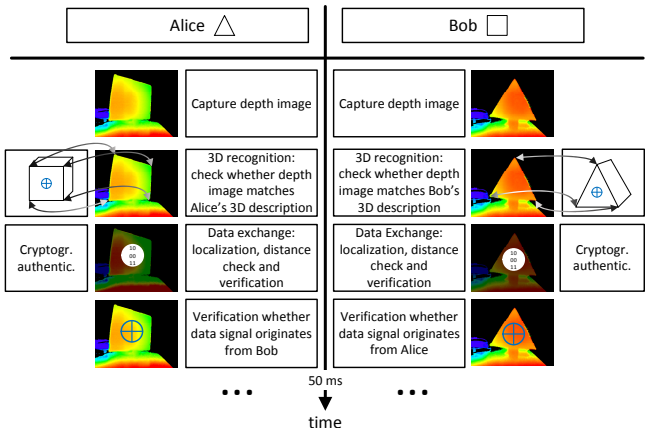

Figure 6. Example of an OptiSec3D secure communication procedure during a certain timeslot.

- Optical communication in conjunction with 3D shape checks (e.g., biometrics such as face recognition and fingerprints) will make authentication-based applications more secure against spoofing attacks.
- OptiSec3D's unique union of optical communication and 3D sensing will represent a key enabling technology and will open whole new fields of applications (such as long-distance secure pairing of devices by pointing towards the communication partner).

Figure 5 depicts a proposed OptiSec3D communication node from a design perspective. It consists of the Time-of-Flight unit, which is made of the illumination and the sensor units, a micro-controller (or FPGA), and a security anchor given as a secure element. On the one hand, the micro-controller implements Time-of-Flight specific algorithms (such as processing of exchanged data, calculating 3D depth data from raw sensor data, distance and area verifications) and the protocols to the attached embedded system. On the other, the secure element implements security related functionality (such as encryption, decryption, authentication protocols, key handling). Thus, a modular and secure communication technology will be given that can be easily integrated or plugged into embedded systems.

3.3 OptiSec3D-based Secure Authentication

OptiSec3D supports several possibilities to implement secure authentication methods. As a fundamental feature, two Time-of-Flight communication partners easily detect each other through very distinctive amplitude as well as depth values (exemplified by white circuits in Figure 6 and demonstrated in Figure 9) within the sensed 3D-scenery. These values are highly local and are caused by the Time-of-Flight illumination unit. Thus, 3D localization (relative position, distance, etc.) of the communication partner is achieved with little effort. After the communication partner was detected, the authentication procedure can start. To outline some examples, following approaches are feasible.

First, the Time-of-Flight optical communication channel can be used to implement typical asymmetric authentication methods, such as elliptic-curve based cryptography.

Second, the communication partners use the optical Time-of-Flight channel to transmit not only data but also the measured distances. This distance information can then be used by the communication partners to decide, e.g., whether general Time-of-Flight optical communication between both partners is continued, or the authentication procedure is started, etc.

Third, a Time-of-Flight system can use 3D information stored in a database to compare it with the sensed 3D data. Thus, it is able to recognize the communication partner (e.g., a car, a payment terminal, or a human's biometric information). It is possible to finish the recognition in a very small time interval, which makes it possible to re-authenticate the communication partner multiple times per second. Figure 6 shows a basic example for a secure communication flow employing the Time-of-Flight technology. The procedure in the figure is performed multiple times per second. For example, the majority of secure authentication use-cases features at least one communication partner with static appearance. An example would be a reader at a payment terminal. This known and unchangeable geometry can be stored and provided as a library of 3D datasets. The necessary algorithms to match a depth image with an existing dataset are well established and can be executed in the required timespan.

3.4 Counter Measure against Relay Attacks

Relay attacks are very severe in the RF domain. In the Time-of-Flight domain, distance, 3D localization, shape of the communication partners, and 3D-origin of the communication are known. Furthermore, the Time-of-Flight communication partners use an optical line-of-sight connection. These key-features make security attacks difficult to implement. If, for example, a relay-attacker managed to get into the field-of-view of a Time-of-Flight communication system, he would have to reproduce the exact distances (an authentication only succeeds if both communication partners measure the same distance) between the communication partners. This is outlined in Figure 7. In combination with state-of-the-art security features (message authentication, encryption, authentication protocols, etc.) and the Time-of-Flight's location awareness (communication partners sense depth images of each other and have exact knowledge from which direction and distance the signal of the communication partner originates), further crucial security barriers are given. These security features make it very difficult for attackers, even

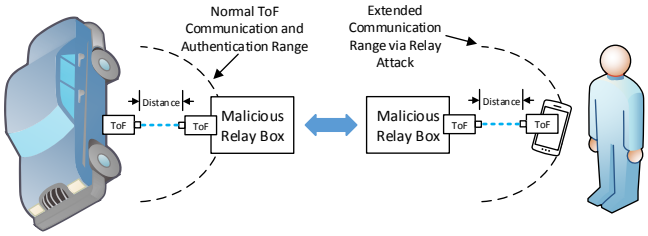

Figure 7. Theoretical concept for a Time-of-Flight based relay attack.

practically impossible, to intercept communication, to spoof distance information, and to maliciously relay the communication. The outlined security measures can be carried out multiple times per second and are thus robust against communication partners in motion. Furthermore, the computation and verification tasks can be done in parallel and do not halt or delay communication.

4 System Prototype and Results

In order to proof the feasibility of the OptiSec3D concept, a very first prototype system was developed. Figure 8 shows the basic approach. Two Infineon REAL3™ sensor evaluation boards, which are based on Time-of-Flight technology of pmdtechnologies, are facing each other. A common clock source is provided to the sensors, in order to avoid carrier detection and clock synchronization issues. Both evaluation boards are connected to a PC through USB 3.0. Matlab is used to configure the cameras, to process the data, and to evaluate the results.

4.1 Depth Sensing and Detection of Devices

A very important requirement is to ensure an easy detectability of transmitting communication partners within the 3D environment. For this detectability test, the two evaluation boards of the prototype system were operated in depth-sensing mode employing the same modulation frequency (but without synchronization). Figure 9 shows Time-of-Flight amplitude and depth data that displays the Time-of-Flight communication partner (implementing two illumination LEDs) mounted on a wooden fixing. Within the left images, the communication partner has its illumination LEDs

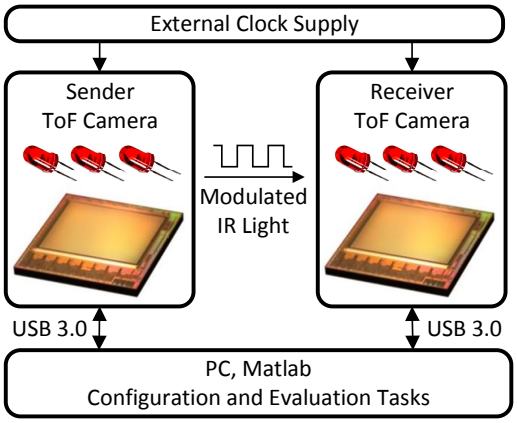

Figure 8. Proposed OptiSec3D communication interface.

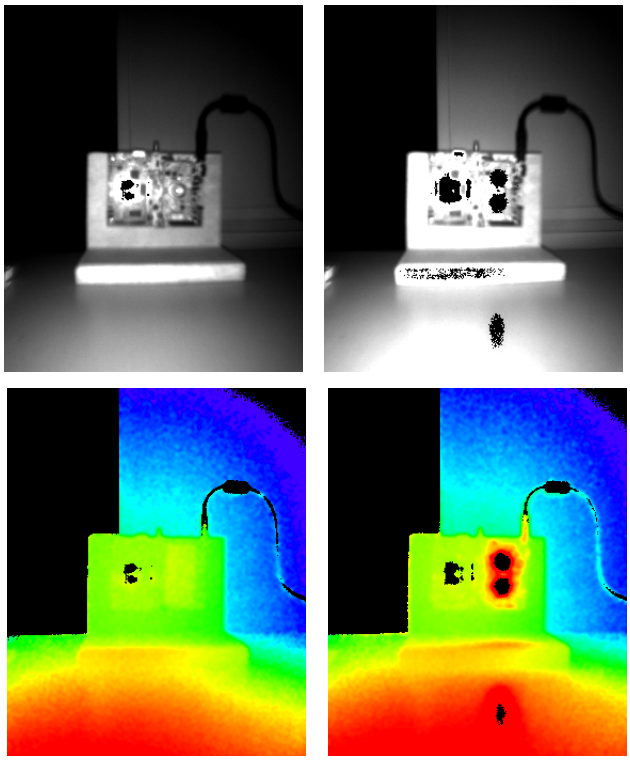

Figure 9. Time-of-Flight amplitude and depth data showing another camera with deactivated illumination (left image) and activated illumination (right image).

deactivated. Whereas, within the right images, the communication partner has its illumination LEDs activated. Thanks to this local and very distinctive amplitude and depth inconsistencies, an OptiSec3D device is able to detect other transmitting communication partners in the 3D environment with only little effort.

4.2 Optical Data Transfer

Successful data transfer between Infineon's REAL3™ evaluation boards can be practically achieved through various approaches. In the following, two implementations are exemplarily presented.

In the first approach, the sender camera emits modulated light with a phase of, e.g., 0° and 180°. The receiving camera samples with a higher frequency and evaluates the Time-of-Flight pixels' raw data. No depth or amplitude images are calculated (cf. Figure 1). The visualization of the sensed raw data is given by Figure 10. One can easily detect the two raw data peaks, which prominently stand out from the noise-level, and which are caused by the two illumination LEDs of the sender. Given this behavior and by considering a Time-of-Flight system's characteristics, one can implement a basic Time-of-Flight-based communication system by evaluating the sensed raw data only.

In the second approach, a higher order modulation scheme is demonstrated, such as an 8-PSK. For this purpose, the receiving device now implements a proper sampling and phase calculation method. The transmitted phase and amplitude information is sampled four times and calcu-

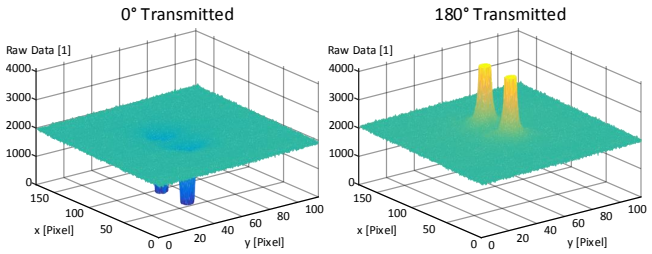

Figure 10. Sensed raw data of the sender who transmits light with 0°(left image) and 180°(right image) phase shift.

lated according to Equation (1) and (2) by the receiver. Thus, a more robust communication can be achieved that also provides higher data rates. For demonstration purposes, Figure 11 depicts the sensed and calculated phase images on receiver side.

$$\varphi = \arctan\left(\frac{A_{90^\circ} - A_{270^\circ}}{A_{0^\circ} - A_{180^\circ}}\right) \quad (1)$$

$$A = \frac{\sqrt{(A_{90^\circ} - A_{270^\circ})^2 + (A_{0^\circ} - A_{180^\circ})^2}}{2} \quad (2)$$

5 Conclusion

Information security is a major challenge in today's interconnected world. Recent concepts, such as the Internet-of-Things, further intensify the need for secure information and communication technologies as well as dedicated hardware security which is hardened against all kinds of security attacks.

This paper introduces OptiSec3D, a new approach for secure information and communication systems. OptiSec3D uniquely enhances the key enabling Time-of-Flight 3D localization technology with optical communication abilities and state-of-the-art security anchors. Thus, new levels of trust and security can be reached for information and communication systems. This work demonstrates OptiSec3D's feasible implementation with the help of a very first prototype. Furthermore, it shows how the OptiSec3D technology can counteract sever security attacks, such as relay attacks.

Our future work concerns the development of an OptiSec3D communication node that also employs dedicated hardware security (i.e. security controllers) for security-critical applications.

6 Acknowledgments

The authors would like to thank the Austrian Federal Ministry for Transport, Innovation and Technology as well as the ARTEMIS Joint Undertaking, which funded the research activities under the grant agreement n° 852328 and n° 621429 respectively.

7 References

[1] S. Brands and D. Chaum. Distance-bounding Protocols. In *Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology (EUROCRYPT)*, pages 344–359, 1994.

[2] C. Cremers, K. Rasmussen, B. Schmidt, and S. Capkun. Distance Hijacking Attacks on Distance Bounding Protocols. In *IEEE Symposium on Security and Privacy (SP)*, pages 113–127, May 2012.

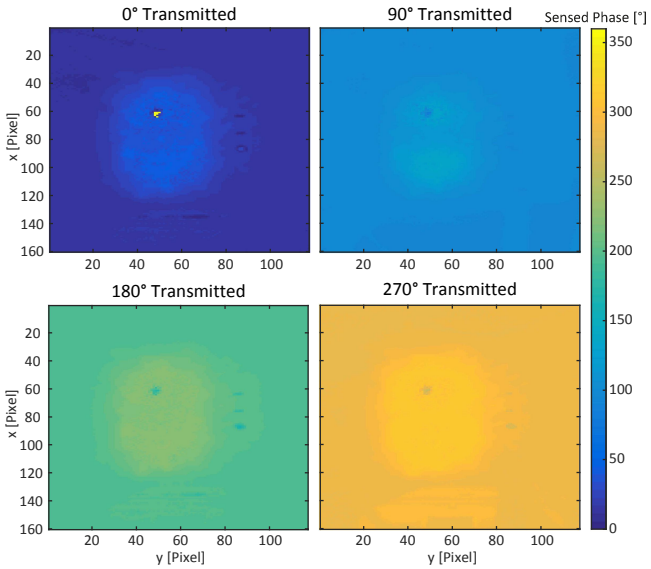

Figure 11. Sensed and calculated phase data of the sender who transmits data symbols of, e.g., 0°, 90°, 180°, and 270° phase information.

[3] N. Druml, G. Fleischmann, C. Heidenreich, A. Leitner, H. Martin, T. Herndl, and G. Holweg. Time-of-Flight 3D Imaging for Mixed-Critical Systems. In *13th International Conference on Industrial Informatics (INDIN)*, pages 1432–1437, July 2015.

[4] K. Finkenzeller. *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*. John Wiley & Sons, Inc., New York, NY, USA, 2 edition, 2003.

[5] A. Francillon, B. Danev, and S. Capkun. Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars. In *Network and Distributed System Security Symposium (NDSS)*, February 2011.

[6] G. Hancke and M. Kuhn. An RFID Distance Bounding Protocol. In *First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SecureComm)*, pages 67–73, September 2005.

[7] E. Haselsteiner and K. Breitfu. Security in Near Field Communication (NFC). Strengths and weaknesses. In *Workshop on RFID Security*, 2006.

[8] M. Hutter, J.-M. Schmidt, and T. Plos. RFID and Its Vulnerability to Faults. In *Proceedings of the 10th International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, 2008.

[9] J. Krissler. Ich sehe, also bin ich ... Du. Gefahren von Kameras für (biometrische) Authentifizierungsverfahren, 2014.

[10] R. Lange and P. Seitz. Solid-state time-of-flight range camera. *IEEE Journal of Quantum Electronics*, 37(3):390–397, March 2001.

[11] S. Prabhakar, S. Pankanti, and A. Jain. Biometric recognition: security and privacy concerns. *Security Privacy, IEEE*, 1(2):33–42, March 2003.

[12] S. Ravi, A. Raghunathan, P. Kocher, and S. Hattangady. Security in Embedded Systems: Design Challenges. *ACM Transactions on Embedded Computing Systems (TECS)*, 3(3):461–491, August 2004.

[13] N. Savage. Li-Fi gets ready to compete with Wi-Fi. *Spectrum, IEEE*, 51(12):13–16, December 2014.

[14] J. Y. Wang. Imaging laser radar - An overview. In R. W. McMillan, editor, *Lasers '86; Proceedings of the Ninth International Conference on Lasers and Applications*, pages 19–29, 1987.

[15] Z. Xu, T. Möller, H. Kraft, J. Frey, and M. Albrecht. Photonic mixer device, April 2008. US Patent 7,361,883.

[16] W. Yuan, R. Howard, K. Dana, R. Raskar, A. Ashok, M. Gruteser, and N. Mandayam. Phase messaging method for time-of-flight cameras. In *IEEE International Conference on Computational Photography (ICCP)*, May 2014.