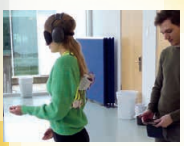
Institut für Angewandte Forschung Hochschule Offenburg

forschung im fokus

Ausgabe Nr. 22 / 2019



Assistenztechnologien & Emotionen: scheinbar Gegensätzliches

Aerodynamische Optimierung eines Leichtbaufahrzeugs

ivESK – INSTITUT FÜR VERLÄSSLICHE EMBEDDED SYSTEMS UND KOMMUNIKATIONSELEKTRONIK

Das „Internet der Dinge“ (Internet of Things, IoT) durchdringt zunehmend industrielle und persönliche Anwendungen. Hierzu zählen beispielsweise Smart-Metering und Smart-Grid, Industrie- und Prozessautomation, Car-to-Car, bzw. Car-toX-Kommunikation, Heim- und Gebäudeautomation, Telehealth- und Telecare-Anwendungen. Die drahtgebundene und drahtlose Vernetzung von Embedded Systemen und deren Anbindung als sogenannte cyberphysische Systems (CPS) spielen hierbei eine immer wichtigere Rolle. Da auch immer mehr Systeme funktionskritische Aufgaben autonom übernehmen, gewinnen Zuverlässigkeit und Sicherheit immer mehr an Bedeutung. Entsprechend müssen die Aspekte der Datensicherheit und der Privatsphäre (Privacy) ebenfalls und von Anfang berücksichtigt werden.

Diesen Themen widmet sich das Institut für verlässliche Embedded Systems und Kommunikationselektronik (ivESK) an der Hochschule Offenburg, das im Herbst 2015 von Prof. Dr.-Ing. Axel Sikora und Prof. Dr. rer.nat. Dirk Westhoff gegründet wurde und das sich seither außerordentlich positiv entwickelt hat. Es werden pro Jahr etwa 20 F&E-Projekte in enger Kooperation mit Unternehmen und anderen Forschungseinrichtungen bearbeitet, um das Internet der Dinge zuverlässiger und verlässlicher zu machen.

Am Institut arbeiten gegenwärtig 12 VollzeitmitarbeiterInnen sowie etwa ebenso viele Studierende. Aufgrund der sehr positiven Projektlage sind noch einige Projekt- und Promotionsstellen offen. Kandidaten für Tutorentätigkeiten und Abschlussarbeiten sind gern gesehen.

https://ivesk.hs-offenburg.de

Institutsleitung
Prof. Dr.-Ing. Dipl.-Ing. Dipl.-Wirt.-Ing. Axel Sikora

Unified Performance Analysis of LPWAN based Smart Waste Management System

Jubin E. Sebastian M.Tech, Dipl.-Infom. (FH) Manuel Schappacher, Prof. Dr.-Ing. Dipl.-Ing. Dipl.-Wirt.-Ing. Axel Sikora

Das Internet der Dinge (Internet of Things, IoT) setzt eine zuverlässige und flexible, oft drahtlose Kommunikation voraus. Der Test räumlich verteilter Funksystemen bringt hierbei besondere Anforderungen mit sich. Der Beitrag stellt eine am Institut der Autoren entwickelte durchgängige Testumgebung zur Durchführung systematischer Tests vor und berichtet über die Messergebnisse für Low-Power-Wide-Area-Netzwerke (LPWAN) für den Anwendungsfall intelligenter Müllbehälter.

To enable megatrends like Internet of Things (IoT) reliable wireless communication technologies play a major role. Spatially distributed wireless technologies introduce additional challenges in testing. This article describes the overall architecture of a unified test environment and provides an overview of the performance investigations of various Low-Power-Wide-Area network (LPWAN) technologies for a smart waste management use case.

Introduction

In the age of Internet of Things (IoT) and Industry 4.0, practically all industrial application fields are affected from the increasing trend of digitization and networking. With this "megatrend", applications and devices are being digitized and integrated into the intelligent exchange of information. Many smart world use cases are addressed like home and building automation, industrial and process automation, vehicle and traffic engineering, logistics, safety technology, power engineering or medical technology (Telehealth, Telecare) and many more. The main motivation for this trend is that with the networked application the system efficiency can be increased, and costs can be saved. Also new applications, business or service models are possible. Many of these use cases are enabled by spatially distributed networking solutions which use wireless communication channels. To ensure reliable performance, testing and performance measurements need to be performed during the development, the installation and the deployment phases.

For the entire development process of wireless communication systems, the Institute of Reliable Embedded Systems and Communication Electronics (ivESK) at Offenburg University [1] follows a continuous test-driven design flow for distributed communication nodes. It includes various abstraction levels and is based on identical software or firmware implementations and identical test cases at these levels. These testing approaches range from simulation over virtualization and emulation of the network to field tests. In a recent research project, ivESK together with Binando GmbH [2], a young enterprise developing a platform for intelligent waste collection, have performed a systematic performance analysis of innovative long-range low-power wireless communication technologies like Low-Power Wide-Area Networks (LPWAN) or Narrowband IoT (NB-IoT) using this test environment.

Smart Waste Management Use Case

With smart city use cases companies and government try to address efficient and intelligent utilization of resources and to overcome challenges of surging population growth and urbanization. The use case example of smart waste management system is considered in this article, which deal with the ever-increasing amount of garbage in cities and in the collection of recyclables. This area of application promises significant efficiency gains through the monitoring of collection points or containers and optimization in the route planning of collection vehicles. The Binando GmbH is a young enterprise, which in co-operation with the energy supplier EnBW developed the platform for intelligent waste collection. The platform offers basic solutions from hardware including maintenance through software to a cloud-based dashboard and already covers all the required elements of an overall system. A sensor was specially designed and developed for waste containers which measures the level in one garbage containers, such as a glass or

Fig. 1: Binando smart dustbin

a paper container, and sends the levels and other data like temperature or humidity regularly to the backend. One to the needs of waste management tailored route planning based on the current and predicted levels of the container, which allows an optimized route while preventing overfilled containers. A dashboard provides insights into the valuable information of containers and routes. It exists also the possibility to set up notifications for special events, to export the data or to be given specific recommendations for action [2].

The connection of the sensors in the spatially distributed waste containers has so far been carried out with the help of cellular mobile communication (GSM / GPRS, or UMTS). This approach is functional and simple, but the requirements to connect many spatially distributed low-power sensor devices at low cost, with low energy consumption are some of the challenges yet need to be addressed.

Low-Power Wide-Area Networks (LPWAN)

A low-power wide-area network (LPWAN) is a novel type of wireless communication wide area network designed to allow long range communication to interconnect low-bandwidth and battery-powered devices (connected objects), such as sensors. LPWANs promise a new level of link budgets at low output power and cost allowing a long range and stable local communication in IoT deployments. LPWAN is not a single technology, but it is the common name of various low-power, wide-area network technologies, with different building blocks.

In general, LPWANs may operate in unlicensed and licensed bands. The networks operate in unlicensed bands are kind of ad-hoc network and proprietary solutions are already available in the market such as LoRa/ LoRaWAN, SigFox, and MIOTY. LoRa/LoRaWAN [1] is based on chirp spread spectrum (CSS) radio modulation technology, SigFox [2] is based on Ultra Narrow Band (UNB) modulation technology, and MIOTY [3] is empowered with telegram splitting technology. Licensed LPWANs are cellular network variants, being standardized by 3GPP under the umbrella term of cellular IoT (cIoT). The most suitable cIoT technology for LPWAN use case is Narrow Band IoT (NB-IoT). The narrowband versions of cellular technology approaches are with reduced bandwidth and simplified node and network management mechanisms [12].

We fundamentally know that for radios in long range we can either increase the transmission power or to decrease the bandwidth of the channel. LPWAN technologies combine low-energy operation of wireless systems with low data-rate and bandwidth. They enable excellent receiver sensitivities of as low as -150 to -160dBm to achieve link budgets of 160 to 170dB with output power of as low as 10dBm. Thus, they reach distances of several (typically around 10) kilometres. They are also very economic both in device cost (investment cost) and in complexity of network management (operational cost). Combining these features, they enable a new class of applications for the Internet of Things (IoT), which requires low data-rate, simple, long-range, low-energy for battery powered or energy-autarkic operation.

Since these LPWAN use cases come with various requirements in terms of RF coverage, energy, complexity, scalability, autonomy and cost, it is essential to perform a comparative analysis of competing technologies. In this project, we systematically compared the different available technology choices for spatially distributed connectivity, according to the radio scheme and other sensor device specific requirements of binando GmbH. The ivESK team conducted a systematic test campaign with identical test cases to measure and compare the performance of various technologies.

Challenges in testing of spatially distributed wireless communication technologies

Testing of spatially and functionally distributed wireless networking solutions can't be covered by conventional testing methods. These wireless networks introduce a multitude of different test scenarios. Testing such systems are always complex due to the short-lived nature of wireless signal propagation, irreproducible channel characteristics, various network topologies etc. Testing and validation of these technologies are essential before the deployment. Most of the existing testing solutions are platform specific. It is particularly important in such complex systems to test individual components that are as clear and independent as possible at an early stage, and only then, once their correct function has been verified, to test the entire system. This procedure considerably reduces the effort for troubleshooting and increases test coverage and thus reliability. Testing of wireless systems are performed in various abstraction levels such as network simulation, virtualization, emulation, and field tests in the state of the art. Until today, test cases are modelled differently at the different levels, even if they describe the same functions or processes [12].

Unified Testing Approach of ivESK

For performing the automated testing of wireless communication and to measure the network performance and stability of wireless networks, a unified testbench has been developed at ivESK. For the entire development process, ivESK follows a continuous test-driven design flow for the distributed communication nodes, which includes various abstraction levels with identical software or firmware implementations and identical test cases.

The basic idea of this universal testbench is to have a unified and seamless test environment for a broad variety of wireless technologies. The unified testbench is realized using three different levels such as test case descriptions and automated execution tools, in various abstraction levels using identical measurement, and analysis tools. An overview of our unified LPWAN and NB-IoT test environment is shown in Fig. 2.

Performance Measurements of LPWAN & NB-IoT

To systematically compare the competing technologies, identical test cases are used in the identical test environment. The test cases are RF coverage, signal quality, packet loss rate, payload flexibility, stability, interference tolerance etc. An Eclipse Titan TTCN-3 based test case de-

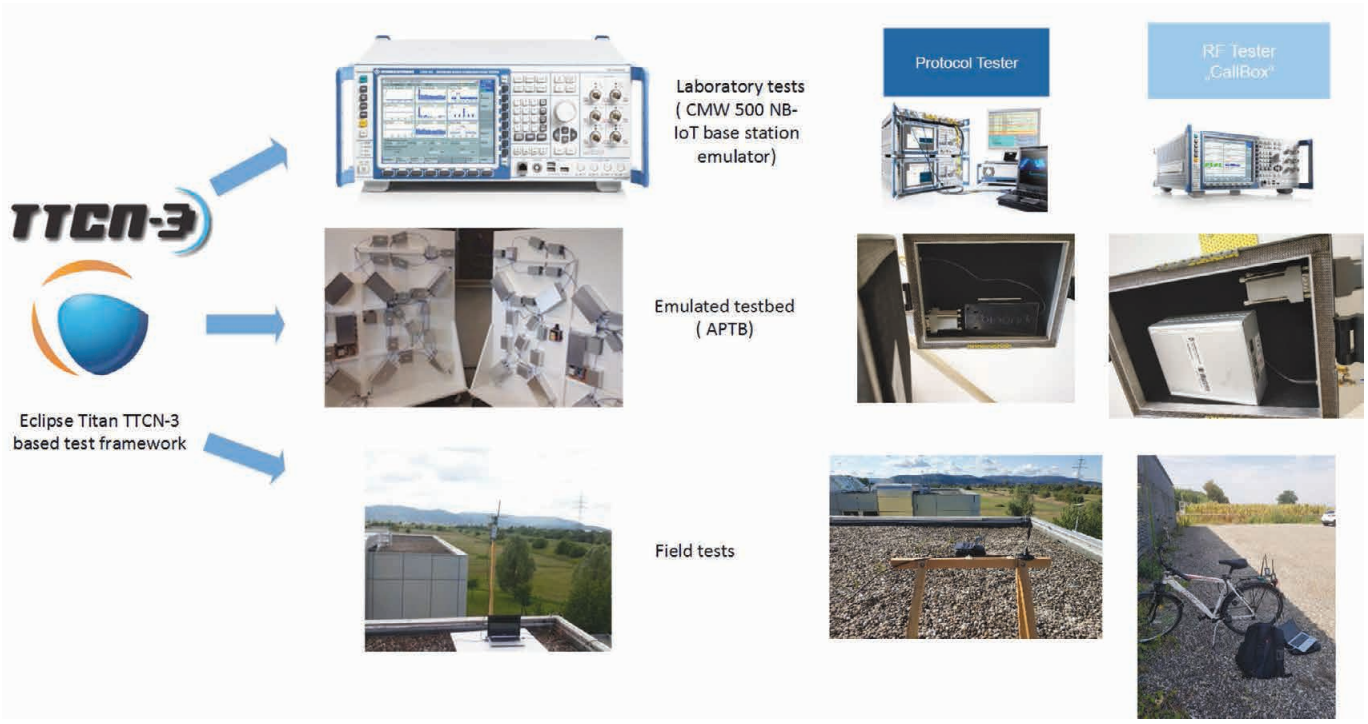
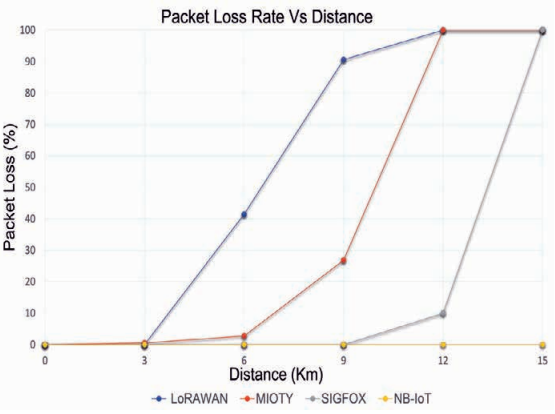


Fig. 2: Unified test environment overview

scription and automated execution framework are also integrated to our test environment [11].

Performance measurements are performed for various tests in laboratory and in field. For RF coverage, payload flexibility, stability and co-existence behavior test cases statistics such as the Received Signal Strength Indication (RSSI), Signal to Noise Ratio (SNR), number of sent and received packets and timing are measured. In this contribution, we provide an overview of performance measurement results from various test campaigns. A performance measurement example from our lab test and field test campaign is given in Fig. 3, on top is the comparison of packet loss from our field measurements and bottom is the throughput measurements in the lab tests.



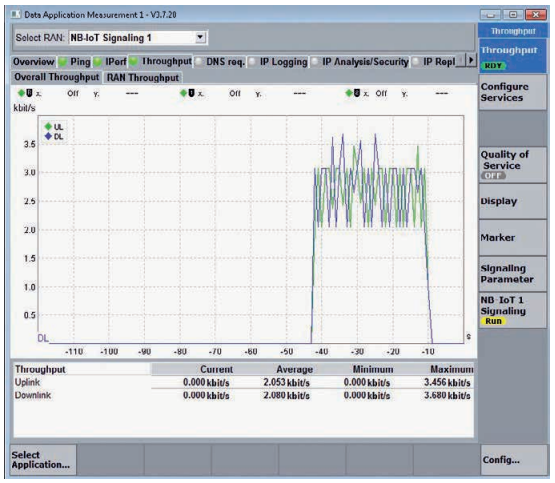


Fig. 3:
Example performance measurements

Summary and Outlook

The tests and performance measurements performed on various technologies confirmed its applicability for smart waste management use case of Binando GmbH in our lab and field measurements with respect to its long range, link budget, payload flexibility, data rate and interference tolerance of these technologies for the use cases considered. With regards to RF coverage the three unlicensed LPWAN technologies are performed well in distances of up to 10 km, with SigFox showing the best penetration in the LPWAN segment. But when it comes to payload flexibility, LoRaWAN was able to handle up to 256 bytes per message, where SigFox can support only 12 bytes and a maximum of 140 messages per day. With regard to the interference tolerance and coexistence issues LoRaWAN showed weaker performance in the field with more lost packets, whereas SigFox and MIOTY performed well. Regarding interference tolerance, MIOTY Telegram Splitting Multiple Access technology [3] proved its capability in our measurements. The NB-IoT technology is getting more attraction due to an attractive data rate (~ 100 kbps), low latencies (~ 1 s), new proposals for in 3GPP Rel.14 for reduced power consumption and upcoming world-wide deployment. When choosing the right technology, we need to also consider trade-off between payload flexibility, interference robustness, and energy consumption. Our systematic comparison using this unified test environment showed the value of such a unified and seamless test & performance measurement environment for comparison of competing spatially distributed wireless networking technologies. Further measurement campaign will follow.

AUTOREN

Jubin E. Sebastian M.Tech.
Doktorand ivESK
sebastian.jubin@hs-offenburg.de

Dipl.-Infom. (FH) Manuel Schappacher
Wissenschaftlicher Mitarbeiter ivESK
manuel.schappacher@hs-offenburg.de

Prof. Dr.-Ing. Axel Sikora
Wissenschaftl. Leiter ivESK, Lehrgebiete: Kommunikationsnetze, Bussysteme und Schnittstellen, eingebettete u. industrielle Netzwerke
axel.sikora@hs-offenburg.de

Referenzen/References:
[1] The Institute of Reliable Embedded Systems and Communication Electronics, https://ivesk.hs-offenburg.de/
[2] Binando GmBH, https://binando.com/
[3] LoRa Alliance, https://www.lora-alliance.org/
[4] SigFox, https://www.SIGFOX.com/en
[5] MIOTY, https://www.iis.fraunhofer.de/de/ff/lv/net/tech/telemetrie.html
[6] 3GPP release for Cellular IoT, http://www.3gpp.org/specifications/releases
[7] A. Sikora, E Jubin Sebastian, A. Yushev, E. Schmitt, M. Schappacher, „Automated Physical Testbeds for Emulation of Wireless Networks", ICMIE 2016, 75, 06006 (2016), pp.1-5, http://dx.doi.org/10.1051/matecconf/20167506006
[8] R & S CMW 500, https://www.rohde-schwarz.com/hu/product/cmw500-pt-product-startpage_63493-10566.html
[9] E. Jubin Sebastian, J.M Jose, M. Schappacher, A. Sikora, „ Seamless test environment for distributed embedded wireless networks", Proc. of the 2017 International Conference on Advances in Computing, Communica-tions and Informatics (ICACCI)Confer-ence (Sept 2017, Udupi, India
[10] A. Sikora, M. Schappacher, A. Yushev, „A Novel Virtualized Testbed for Embedded Networking Nodes (VTENN)", Proc. of the 2017 IEEE International Instrumentation and Measurement Technology Conference (I2MTC), 22-25 May 2017, Torino, Italy, pp. 117-122.
[11] A. Yushev, M. Schappacher, A. Sikora, „Titan TTCN-3 Based Test Framework for Resource Constrained Systems", MATEC Web of Conferences, ICMIE 2016, 65, 06005 (2016), pp. 1-5, http://dx.doi.org/10.1051/matecconf/20167506005
[12] E. Jubin Sebastian, M. Schappacher, A. Sikora, „ Unified Test Environment for LPWAN and Cellular IoT", Accepted for publication in Proc. of the Embedded World Conference, 2019

Integrierte Sicherheit durch Physical Unclonable Functions (PUFs)

Lukas Zimmermann M.Sc., Alexander Scholz M.Sc., Prof. Dr.-Ing. Dipl.-Ing. Dipl.-Wirt.-Ing. Axel Sikora

Die zunehmende Vernetzung eingebetteter Systeme im Internet der Dinge erhöht den Bedarf an kostengünstigen Sicherheitseinheiten für kryptografische Anwendungen, wie beispielsweise für die Verschlüsselung von Kommunikationsdaten oder zur Authentifizierung einzelner Geräte. Sogenannte Physical Unclonable Functions (PUFs) versprechen eine sichere Möglichkeit, unkontrollierbare intrinsische Variationen zur Generierung einzigartiger Erkennungsmerkmale (IDs) zu nutzen.

The increasing interconnection of embedded systems in the Internet of Things (IoT) calls for low-cost security primitives for cryptographic applications. Examples are the encryption of data in transport or the authentication of unique devices. So called Physical Unclonable Functions (PUFs) promise a secure possibility to leverage from uncontrollable process-dependent intrinsic variations to generate unique identifiers (IDs).

Einleitung

Vernetzte eingebettete Systeme prägen seit Jahren unseren Alltag. Unabhängig von der Anwendung agieren sie meist im Hintergrund und sind für den Nutzer unsichtbar. Die möglichen Einsatzgebiete sind breit gestreut und umfassen beispielsweise die Gebäude-, Industrie- und Prozessautomatisierung, Fahrzeugbau, Logistik, Energieversorgung, Medizin und viele mehr. Dabei spielt auch der Trend hin zum Internet of Things (IoT) eine immer größere Rolle. Bisher isolierte Geräte werden miteinander vernetzt, die dann ohne Zutun eines menschlichen Akteurs miteinander kommunizieren. Deshalb müssen besonders Sicherheitsaspekte wie verschlüsselte drahtlose oder drahtgebundene Kommunikationen berücksichtigt werden. Vor allem eingebettete Systeme mit eingeschränkten Ressourcen, wie sie oft in Low-Cost-Applikationen zum Einsatz kommen, sind signifikanten Risiken ausgesetzt und werden auch immer öfter zum Einfallstor für Angriffe.

Softwarebasierte Sicherheitslösungen allein können die Integrität des Gesamtsystems nicht sicherstellen [1]. Da potenzielle Angreifer in vielen Fällen physischen Vollzugriff auf ein eingebettetes System erreichen können, besteht die zusätzliche Gefahr, dass die Integrität der Firmware nicht mehr gewährleistet werden kann und ggfs. Duplikate entstehen. Aus diesem Grund werden oft in Hardware implementierte Sicherheitserweiterungen integriert, auf die das Gesamtsystem aufbauen kann. Diese bieten einen eindeutigen Identitätsnachweis in Form einer Identifikationsnummer (ID), die für kryptografische Anwendungen oder zur Identifizierung und Authentifizierung eingesetzt werden können. Ein mögliches kostengünstiges Sicherheitsmerkmal bieten Physical Unclonable Functions (PUFs), die man als Speicher für kryptografische Schlüssel einsetzten kann [2]. PUFs sind physikalische Objekte, meist in Form einer elektronischen Hardwareschaltung umgesetzt, die durch die Variationen in ihrem Herstellungsprozess eindeutige Merkmale erhalten. Nach dem Anlegen eines Stimulus, einer sogenannten Challenge, antwortet eine PUF mit einem zufällig aussehenden, aber reproduzierbaren Signal, der sogenannten Response. Diese Response kann beispielsweise als kryptografischer Schlüssel oder als Identifier verwendet werden.

Grundlegendes PUF Konzept

Die grundlegende Idee von PUFs besteht darin, intrinsische Variationen, die, durch den Herstellungsprozess bedingt, jedoch nicht von diesem gezielt beeinflussbar sind, zu nutzen. Dies ermöglicht es, eindeutige und zufällige Erkennungsmerkmale vergleichbar mit dem menschlichen Fingerabdruck zu generieren. Einer der Vorteile besteht darin, dass die daraus resultierende digitale ID nicht vom Hersteller beeinflusst oder zu einem späteren Zeitpunkt von einem Angreifer verändert werden kann.

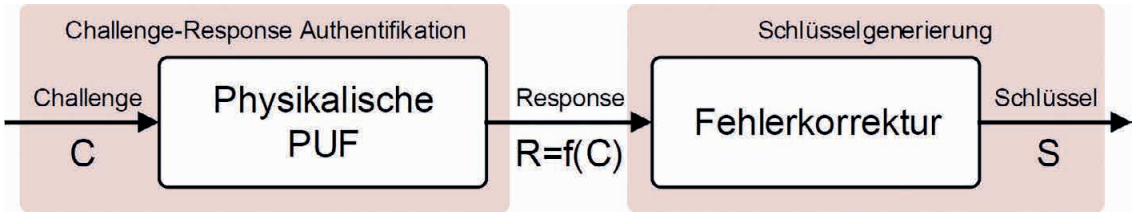


Abb. 1:
PUF-Architektur

Im Allgemeinen kann eine PUF als physikalische Struktur beschrieben werden. Im Speziellen verhält sich eine PUF wie eine Einwegfunktion in Form einer Black Box, die mit einer Challenge C angeregt wird und mit einer Response R antwortet (siehe Abbildung 1).

Aufgrund der intrinsischen Variationen ist die Response nicht vorherzusehen. Mit steigender Komplexität der PUF-Schaltung können höhere Challenge- und Response-Bitbreiten erreicht werden, wodurch der Adressraum vergrößert wird. Es gibt Anwendungen, bei denen es Sinn macht, eine PUF nicht komplett auszulesen, d. h. nicht die maximale Challenge-Bitbreite zu nutzen, sondern den Challenge-Response-Adressraum zu unterteilen. Dadurch wird es z. B. bei einer Authentifizierung möglich, unterschiedliche Challenge-Response-Pairs (CRPs) zu nutzen. Dazu kann der Hersteller nach dem Herstellungsprozess einige CRPs auslesen und abspeichern. Bei der Authentifizierung wird die PUF wieder mit einer der gleichen Challenges angeregt und antwortet mit einer Response. Im Anschluss werden beide CRPs auf Gleichheit untersucht. Da es nicht auszuschließen ist, dass gelegentlich Bit-Fehler in den Responses auftreten, kann an dieser Stelle auch ein Binning-Verfahren (z. B. mit Hamming Distanz) angewendet werden. Um eine PUF direkt für die Schlüsselgenerierung einsetzen zu können, sind zusätzliche Fehlerkorrekturverfahren notwendig, um instabile PUF-Response-Bits zu korrigieren. In den letzten Jahren wurden einige Silizium-basierte PUF-Designs in der Literatur veröffentlicht [3] [4][5][6].

Sicherheitseigenschaften von PUFs

In Abhängigkeit vom angestrebten Einsatzgebiet einer PUF ergeben sich unterschiedliche Anforderungen an die Sicherheitseigenschaften. In der Literatur werden mehrere solcher Eigenschaften beschrieben [1]:

Unvorhersagbarkeit: Das Challenge-Response-Verhalten einer PUF soll nicht vorhersagbar sein. Selbst wenn der Angreifer eine bestimmte Menge an CRPs kennt, sollen keine Korrelationen zu anderen CRPs vorhanden sein.

Robustheit: Diese grundlegende Eigenschaft wird unabhängig von der Zielapplikation von nahezu allen PUFs gefordert. Wird eine PUF mehrmals mit derselben Challenge angeregt, sollte die Response im Idealfall immer die Gleiche sein. In der Realität weisen Responses jedoch Rauschen auf. Dies kann im Fall einer digitalen Response zu Bit-Fehlern führen. Die Fehlerrate sollte soweit wie möglich verringert werden. Dazu können z. B. fehlerkorrigierende Codes zum Einsatz kommen [7]. Zur Robustheit einer PUF gehört ebenfalls, dass die CRPs unter veränderten Umgebungsbedingungen (beispielsweise Schwankungen der Temperatur oder Betriebsspannung) zuverlässig und reproduzierbar extrahiert werden können.

Unkopierbarkeit: Für einen Angreifer sollte es unmöglich sein, eine physische Kopie einer PUF zu erstellen. Daraus ergibt sich die Anforderung, dass die für die Generierung der PUF Responses zugrunde liegenden Variationen möglichst zufällig und unkontrollierbar sein sollten. Oft wird in der Literatur zwischen „weak“ und „strong“ PUF unterschieden [8]. Unkopierbarkeit impliziert an dieser Stelle eine große Anzahl von CRPs (strong), da ein Angreifer sonst (weak) in sehr kurzer Zeit alle CRPs messen und auf einfache Art einen Klon erstellen kann.

Forschungsansatz

In dem Anfang 2017 gestarteten kooperativen Promotionskolleg MERAGEM (Modellierung, Entwurf, Realisierung und Automatisierung von gedruckter Elektronik und ihren Materialien) zwischen der Hochschule Offenburg (Prof. Dr. Jasmin Aghassi-Hagmann, Prof. Dr. Elke Mackensen und Prof. Dr. Axel Sikora) und dem Karlsruher Institut für Technologie (KIT) werden Entwurfs- und Designverfahren für hybride und gedruckte Elektronikkomponenten untersucht. Dabei liegt der Forschungsschwerpunkt auf dem Einsatz von gedruckten Elektronikkomponenten für Systeme des Internet der Dinge. Im Rahmen dieser Arbeitsgruppe wird an einem hybriden PUF-Design gearbeitet, das traditionelle Silizium-basierte und gedruckte Elektronikkomponenten vereint. Link zum Internetauftritt: http://www.meragem.kit.edu/

Referenzen/References:
[1] Katzenbeisser, Stefan, and André Schaller. „Physical Unclonable Functions.“ Datenschutz und Datensicherheit-DuD36.12, 2012
[2] Merli, Dominik, and Georg Sigl. „Physical Unclonable Functions.“ Datenschutz und Datensicherheit-DuD 36.12, 2012
[3] Maiti, Abhranil, et al. „A large scale characterization of RO-PUF.“ Hardware-Oriented Security and Trust (HOST), 2010 IEEE International Symposium on. IEEE, 2010
[4] Morozov, Sergey, Abhranil Maiti, and Patrick Schaumont. „An analysis of delay based PUF implementations on FPGA.“ International Symposium on Applied Reconfigurable Computing. Springer, Berlin, Heidelberg, 2010
[5] Garg, Achiranshu, and Tony T. Kim. „Design of SRAM PUF with improved uniformity and reliability utilizing device aging effect.“ Circuits and Systems (ISCAS), 2014 IEEE International Symposium on. IEEE, 2014
[6] Lofstrom, Keith, W. Robert Daasch, and Donald Taylor. „IC identification circuit using device mismatch.“ Solid-State Circuits Conference, 2000. Digest of Technical Papers. ISSCC. 2000 IEEE International. IEEE, 2000
[7] Yu, Meng-Day, and Srinivas Devadas. „Secure and robust error correction for physical unclonable functions.“ IEEE Design & Test of Computers 27.1, 2010
[8] Herder, Charles, et al. „Physical unclonable functions and applications: A tutorial.“ Proceedings of the IEEE 102.8, 2014
[9] Zimmermann, Lukas, et al. „A hybrid system architecture for the readout of a printed physical unclonable function.“ 2018 International Conference on Electronics Technology (ICET). IEEE, 2018
[10] Maiti, Abhranil, Vikash Gunreddy, and Patrick Schaumont. „A systematic method to evaluate and compare the performance of physical unclonable functions.“ Embedded systems design with FPGAs. Springer, New York, NY, 2013

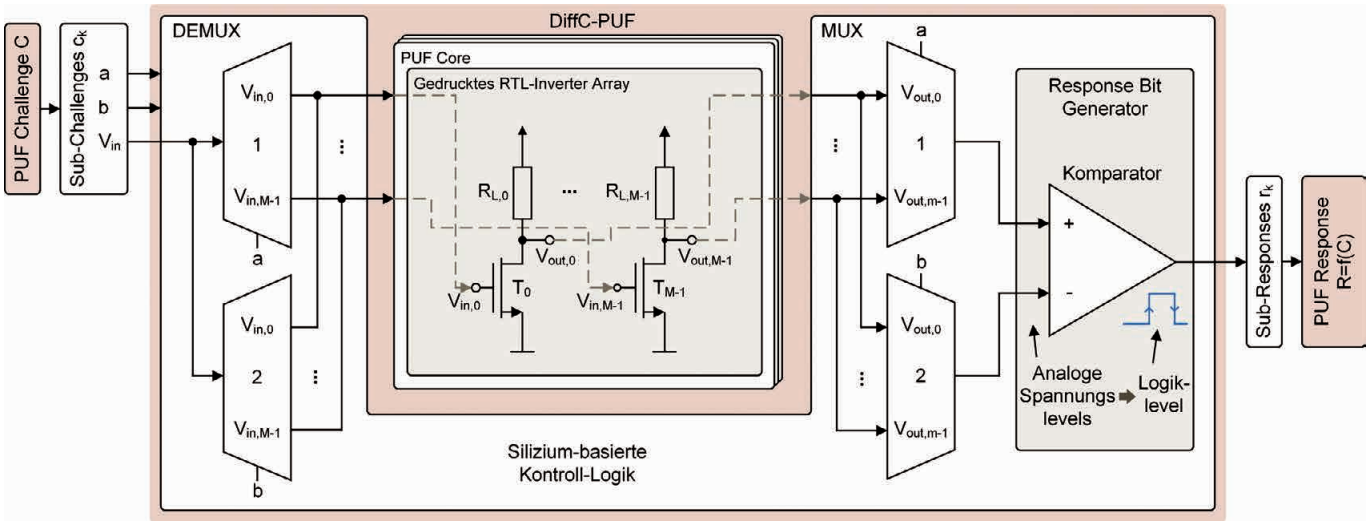


Abb. 2:
Schematische Darstellung der Differential-Circuit- PUF (DiffC-PUF)

PUF Design

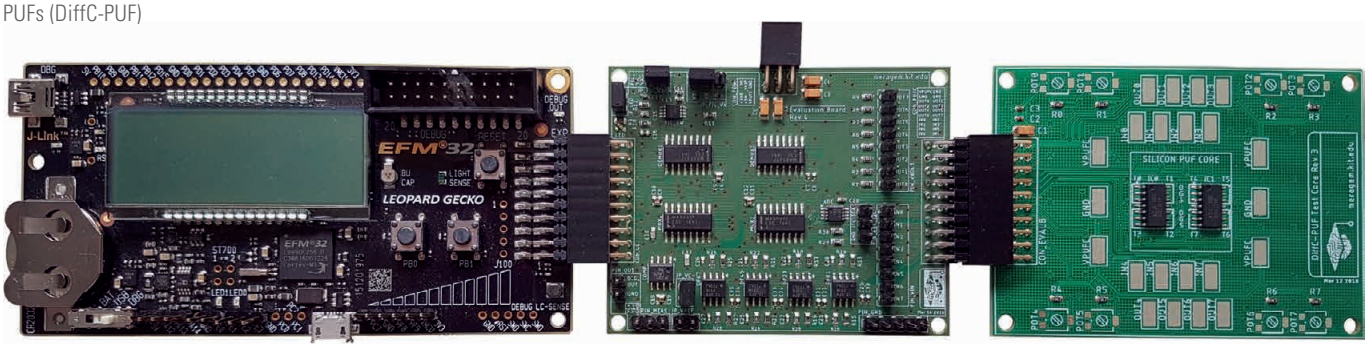
Abbildung 2 zeigt eine schematische Darstellung der im Rahmen dieses Forschungsprojekts entwickelten Differential Circuit PUF (DiffC-PUF).

Die hardwareseitige Umsetzung der DiffC-PUF besteht aus einer Silizium-basierten Steuerungsschaltung, in der die Ansteuerung des gedruckten PUF-Cores realisiert ist. Im Allgemeinen ist der PUF-Core der Schaltungsteil, dessen intrinsische Variationen zur Generierung einzigartiger PUF-Responses ausgenutzt werden. Für die Kontaktierung zwischen den Silizium-basierten und gedruckten Schaltungen kommt eine eigens dafür designte Adapterplatine zum Einsatz. Auf dieser Platine sind spezielle Bonding-Pads vorgesehen, über die durch einen leitfähigen Kleber eine elektrische Verbindung hergestellt werden kann. Das beschriebene Auslese- und Testsystem wird von einem Mikrocontroller gesteuert und kann über eine USB-Schnittstelle von einem Computer aus konfiguriert werden (vgl. Abb. 3) [9].

Simulationsmethodik und Ergebnisse

Im ersten Schritt wurde die Funktionsweise der PUF-Schaltung mit Monte-Carlo-Simulationen verifiziert. Als Grundlage diente ein am KIT entwickeltes Simulationsmodell für Electrolyte-Gated Field Effect Transistors (EG-FETs), die für die reale Umsetzung der PUF-Core-Schaltung eingesetzt werden sollen. Um die Funktionsweise der entwickelten DiffC-PUF nachzuweisen, wurde ein softwarebasiertes DiffC-PUF Emulationsmodell für die Steuerlogik implementiert. In diesem Modell können zusätzliche Störfaktoren simuliert werden, die im realen Betrieb auf den Komparator einwirken. Dadurch sowie unter weiterer Berücksichtigung von unterschiedlichen Betriebstemperaturen kann die Robustheit des DiffC-PUF-Designs untersucht werden. Für die Validierung des Designs wurden die PUF-Metriken Reliability und Uniqueness [10] untersucht (siehe Tab. 1). Die Ergebnisse zeigen, dass sich die DiffC-PUF als zuverlässige und robuste Sicherheitsprimitive eignet. Dabei werden die Vorteile von Silizium-basierten und gedruckten Elektronikkomponenten kombiniert und in Form eines hybriden Gesamtsystems auch für Industrieanwendungen zugänglich gemacht.

Abb. 3:
Hardware zum Testen des Differentia-Circuit-PUFs (DiffC-PUF)



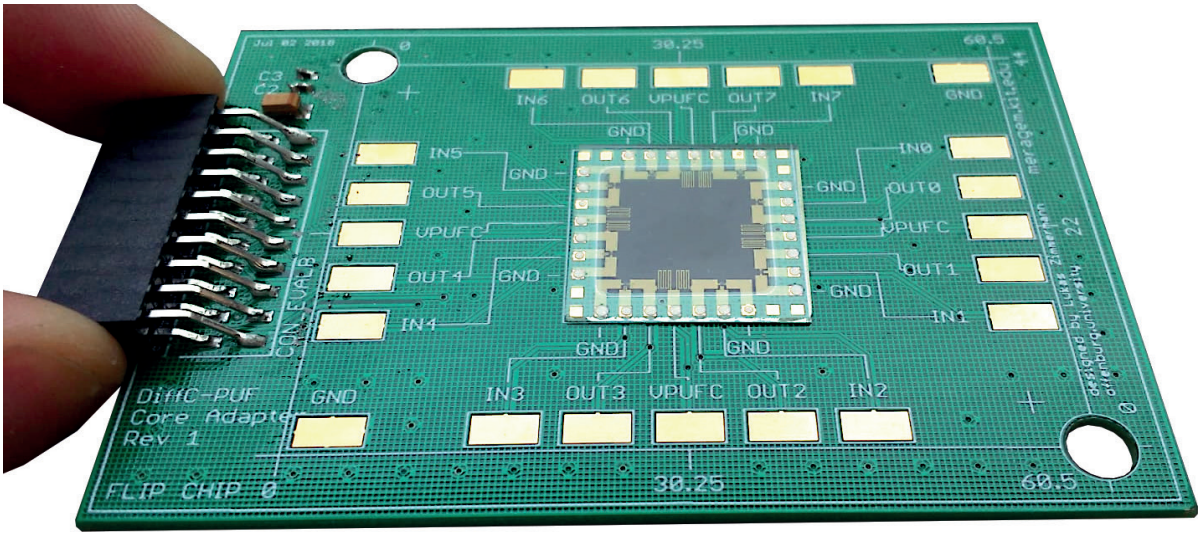


Abb. 4:
Gedruckter Differential-Circuit-PUF-(DiffC-PUF-)Core auf der Adapterplatine

Als Ersatz für den gedruckten PUF-Core wurde ein Silizium-basiertes Pendant entwickelt, das – trotz der um Größenordnungen geringeren herstellungsprozessbedingten Variationen – sehr gute Ergebnisse liefert und durch diskrete Bauteile mit geringem Aufwand in bestehende PCBs integriert werden kann. Tabelle 1 vergleicht die Resultate für die berechneten PUF-Metriken zwischen der gedruckten und Silizium-basierten (experimentelle Ergebnisse) DiffC-PUF.

Zusammenfassung und Ausblick

Im Rahmen des Promotionskollegs wurde eine neue PUF-Architektur entwickelt, die auf einer Kombination von herkömmlicher Silizium-basierter Technologie und gedruckten Elektronikkomponenten basiert. Dabei wurde ein Hardware-/Software-Framework für die Ansteuerung und Evaluierung einer hybriden PUF-Struktur entwickelt. Die grundsätzliche Funktionsfähigkeit des Designs wurde mit Monte-Carlo-Simulationen verifiziert. Darüber hinaus wurden 30 Silizium-basierte DiffC-PUF-Cores hergestellt und evaluiert. Beide Technologien führen zu sehr guten Ergebnissen bei der Auswertung der PUF-Metriken Reliability und Uniqueness (siehe Tabelle 1).

PUF-Metrik	Gedruckter DiffC-PUF-Core (simulationsbasierte Erg.)	Silizium-basierter DiffC-PUF-Core (experimentelle Erg.)	Ideal
Reliability	98,37 %	99,20 %	100 %
Uniqueness	50.02 %	48.84 %	50 %

Tab. 1:
Vergleich der PUF-Metriken zwischen gedrucktem und Silizium-basierten DiffC-PUF-Cores

In zukünftigen Arbeiten soll der gedruckte DiffC-PUF-Core mit der Adapter-Platine verbunden und mit dem im Rahmen dieses Forschungsprojekts entwickelten Testsystems untersucht und ausgewertet werden. Die ersten Schritte dazu wurden bereits gemacht und die einzelnen gedruckten Schaltungsteile händisch vermessen sowie die Funktionsfähigkeit festgestellt (siehe Abbildung 4). Ebenso ist geplant, 2019 das gemeinsame Forschungsprojekt „sichEL“ für die Entwicklung von Silizium-basierter sicherer Elektronik mit dem Institut für verlässliche Embedded Systems und Kommunikationselektronik (ivESK) der Hochschule Offenburg und dem Duisburger Fraunhofer-Institut für Mikroelektronische Schaltungen und Systeme (FhG-IMS) zu starten.

AUTOREN

Lukas Zimmermann, M.Sc.
Doktorand ivESK, MERAGEM
lukas.zimmermann@hs-offenburg.de

Alexander Scholz, M.Sc.
Doktorand, IAF, MERAGEM
alexander.scholz@hs-offenburg.de

Prof. Dr.-Ing. Axel Sikora
Wissenschaftl. Leiter ivESK, Lehrgebiete: Kommunikationsnetze, Bussysteme und Schnittstellen, eingebettete u. industrielle Netzwerke
axel.sikora@hs-offenburg.de