Digital Comprehensive Summaries of Uppsala Dissertations
from the Faculty of Science and Technology 2334

Enabling Scalable Security in Internet of Things

ZHITAO HE

ACTA UNIVERSITATIS
UPSALIENSIS
2023

ISSN 1651-6214
ISBN 978-91-513-1949-0
urn:nbn:se:uu:diva-514996

UPPSALA
UNIVERSITET

Dissertation presented at Uppsala University to be publicly examined in Polhemsalen, Ångströmlaboratoriet, Lägerhyddsvägen 1, Uppsala, Wednesday, 13 December 2023 at 09:00 for the degree of Doctor of Philosophy. The examination will be conducted in English. Faculty examiner: Professor Mário Alves (Politécnico do Porto).

Abstract

He, Z. 2023. Enabling Scalable Security in Internet of Things. *Digital Comprehensive Summaries of Uppsala Dissertations from the Faculty of Science and Technology* 2334. 53 pp. Uppsala: Acta Universitatis Upsaliensis. ISBN 978-91-513-1949-0.

The popular notion of Internet of Things (IoT) implies two salient features: 1. a diversity of small *things*, i.e., constrained devices; 2. their seamless integration with the Internet. Pioneering work in Wireless Sensor Networks (WSNs) have laid a solid technological foundation for autonomous, low power wireless communication among battery-powered, microcontroller-based devices. On the other hand, as devices are being connected to the Internet in large numbers, industry experts and regulators have associated IoT with enormous security risk. Sensitive personal information, highly complex business workflows, and critical infrastructure for public safety are at stake. In this dissertation, we first explore the scalability of IoT. Approaching from the particular angle of radio interference, we study unstable and faulty network behavior when links between low power radios are disrupted. Our low cost and practical interference generation tools fill a gap between protocol design and test. We then underline the threat of novel attacks at the physical layer, which lead to denial of service and battery draining of low power radios. Launched from low cost hardware, the attacks we devise are power-efficient and hard to detect; and they reach longer ranges than jamming. Finally, we take a step closer to realization of secure and large-scale IoT deployment by enabling certificate enrollment, a key component in a public key infrastructure, for small devices. We show that automated enrollment of device certificates becomes feasible when a memory and power efficient IoT protocol stack is leveraged. Spanning between the physical layer and the application layer, our work has enriched the knowledge domain of IoT and advanced the technological frontier of scalable and secure IoT deployment.

Keywords: Internet of Things, Wireless Sensor Networks, Radio Interference, Denial-of-service Attacks, Public Key Infrastructure

Zhitao He, Department of Electrical Engineering, Networked Embedded Systems, Box 65, Uppsala University, SE-751 03 Uppsala, Sweden.

ISSN 1651-6214
ISBN 978-91-513-1949-0
URN urn:nbn:se:uu:diva-514996 (http://urn.kb.se/resolve?urn=urn:nbn:se:uu:diva-514996)

Dedicated to my parents Yaozong and Lijuan, and my wife Bing

Acknowledgment

Personal Acknowledgments

I was indebted to many people during my more than ten years as PhD student, overlapped with my roles as researcher at RISE Research Institutes of Sweden and firmware developer at Assa Abloy.

I would like to express my heartfelt gratitude to my supervisor Prof Thiemo Voigt, who did everything he could to encourage and support me in this long, tortuous intellectual journey. I consider myself extremely fortunate to have had Thiemo in the lead, by my side, and on my back. Among the many things I learned from him, Thiemo's servant style leadership will continue to be a source of inspiration for my future career.

I thank my cosupervisor Dr Shahid Raza, for introducing me to the realm of cybersecurity and providing me with knowledgeable advices. I thank Prof Per Gunningberg, my other cosupervisor, for giving me a warm welcome and smooth induction to the IT department.

My golden years of free intellectual explorations were spent together with former colleagues in the Networked Embedded Systems group at RISE. This was a group of highly talented and dedicated individuals. I stood to gain a lot of knowledge in the company of Nicolas Tsiftes, Niclas Finne, Joakim Eriksson, Joel Höglund, Niklas Wirström, Simon Duquennoy, Luca Mottola, and many others. It was truly a privilege to work with you. Thank you, Nicolas, for helping me write the summary in Swedish.

I also learned a lot from the collaboration and free exchanges with the brilliant PhD students in the IT department, in particular Kasun Hewage, Carlos Pérez-Penichet, Ambuj Varshney, and Frederik Hermans.

I appreciated the curiosity and tolerance shown by my Assa Abloy coworkers from the Pre-Product Innovation Department and the Embedded Department, towards my way of thinking and my sometimes dubious double loyalty to my current and former employers. I thank Tomas Jonsson, my project manager, for entrusting me with adopting some of my previous research to my current work. I thank Joakim Löfgren, my line manager, for expediting the paperwork and enthusiastically cheering me on during my last sprint of writing up this dissertation.

I cannot thank enough my parents, who despite contrasting personalities, raised me with a common, strong conviction that knowledge is the biggest treasure.

I thank my wife Bing, for her love and unwavering support despite having long been disillusioned of my true academic credentials.

I thank all of my coauthors and project partners.

Funding Acknowledgments

I want to extend my gratitude to the following funding agencies that financed my research that led to this dissertation: VINNOVA, the Swedish Agency for Innovation Systems; the European Commission under FP7 and CONET; Uppsala VINN Excellence Center for Wireless Sensor Networks (WISENET); SSF, the Swedish Foundation for Strategic Research; Swedish Energy Agency; and ITEA, the Eureka RD&I Cluster on software innovation and digital transition.

Zhitao He
Stockholm, October 2023

List of Acronyms

6LoWPAN	IPv6 over Low-Power Wireless Personal Area Networks
BLE	Bluetooth Low Energy
CSMA	Carrier Sensing Multiple Access
CBOR	Concise Binary Object Representation
COTS	Commercial Off The Shelf
SoC	System on Chip
CoAP	Constrained Application Protocol
DSSS	Direct Sequence Spread Spectrum
DTLS	Datagram Transport Layer Security
EDHOC	Ephemeral Diffie-Hellman Over COSE
ETSI	European Telecommunications Standards Institute
IETF	Internet Engineering Task Force
IPv6	Internet Protocol Version 6
ISM	Industrial, Scientific and Medical
ITU	International Telecommunication Union
LBT	Listen Before Talk
LLN	Low-power and Lossy Network
LwM2M	Lightweight M2M
MAC	Medium Access Control
MCU	Microcontroller Unit
O-QPSK	Orthogonal Quadrature Phase Shift Keying
OSCORE	Object Security for Constrained RESTful Environments
PHY	Physical Layer
PHR	PHY Header
PKI	Public Key Infrastructure
PPDU	PHY Protocol Data Unit
PSDU	PHY Service Data Unit
RFC	Request for Comment
RPL	IPv6 Routing Protocol for Low-Power and Lossy Networks
SDR	Software Defined Radio
SFD	Start-of-Frame Delimiter
SHR	Synchronization Header
SRD	Short-Range Radios
TSCH	Time Synchronized Channel Hopping
UWB	Ultra Wide Band
WSN	Wireless Sensor Network

List of papers

This thesis is based on the following papers, which are referred to in the text by their Roman numerals.

I Carlo Alberto Boano, Zhitao He, Yafei Li, Thiemo Voigt, Marco Zuniga, and Andreas Willig. “Controllable radio interference for experimental and testing purposes in wireless sensor networks”. In: *2009 IEEE 34th Conference on Local Computer Networks.* IEEE. 2009, pp. 865–872. DOI: 10.1109/LCN.2009.5355013

II Zhitao He and Thiemo Voigt. “Precise packet loss pattern generation by intentional interference”. In: *2011 International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS).* IEEE. 2011, pp. 1–6. DOI: 10.1109/DCOSS.2011.5982225

III Zhitao He and Thiemo Voigt. “Droplet: a new denial-of-service attack on low power wireless sensor networks”. In: *2013 IEEE 10th International Conference on Mobile Ad-Hoc and Sensor Systems (MASS).* IEEE. 2013, pp. 542–550. DOI: 10.1109/MASS.2013.18

IV Zhitao He, Kasun Hewage, and Thiemo Voigt. “Arpeggio: A penetration attack on glossy networks”. In: *2016 13th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON).* IEEE. 2016, pp. 1–9. DOI: 10.1109/SAHCN.2016.7732971

V Zhitao He, Martin Furuhed, and Shahid Raza. “Indraj: digital certificate enrollment for battery-powered wireless devices”. In: *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks (WiSec).* ACM. 2019, pp. 117–127. DOI: 10.1145/3317549.3323408

Reprints were made with permission from the publishers.

Other Peer Reviewed Papers

I co-authored the following peer-reviewed papers, before and during my PhD studies.

- Adam Dunkels, Fredrik Österlind, and Zhitao He. "An adaptive communication architecture for wireless sensor networks". In: *Proceedings of the 5th international conference on Embedded networked sensor systems*. 2007, pp. 335–349
- Thiemo Voigt et al. "Sensor networking in aquatic environments - experiences and new challenges". In: *32nd IEEE Conference on Local Computer Networks (LCN 2007)*. IEEE. 2007, pp. 793–798
- Adam Dunkels, Fredrik Osterlind, Nicolas Tsiftes, and Zhitao He. "Software -based on-line energy estimation for sensor nodes". In: *Proceedings of the 4th workshop on Embedded networked sensors*. 2007, pp. 28–32
- Zhitao He, Adam Dunkels, Thiemo Voigt, and Nicolas Tsiftes. "Rethinking link-level abstractions for sensor networks". In: *2008 Second International Conference on Sensor Technologies and Applications (Sensorcomm 2008)*. IEEE. 2008, pp. 537–542
- Yafei Li, Zhitao He, Thiemo Voigt, and Sanna Leidelöf. "A software radio-empowered sensor network". In: *9th Scandinavian Workshop on Wireless Adhoc Networks (Adhoc'09)*. 2009
- Fredrik Österlind, Adam Dunkels, Thiemo Voigt, Nicolas Tsiftes, Joakim Eriksson, and Niclas Finne. "Sensornet checkpointing: Enabling repeatability in testbeds and realism in simulations". In: *Wireless Sensor Networks: 6th European Conference, EWSN 2009, Cork, Ireland, February 11-13, 2009. Proceedings 6*. Springer. 2009, pp. 343–357
- Nicolas Tsiftes, Adam Dunkels, Zhitao He, and Thiemo Voigt. "Enabling large-scale storage in sensor networks with the coffee file system". In: *2009 International Conference on Information Processing in Sensor Networks*. IEEE. 2009, pp. 349–360
- Carlo Alberto Boano, James Brown, Zhitao He, Utz Roedig, and Thiemo Voigt. "Low-power radio communication in industrial outdoor deployments: The impact of weather conditions and ATEX-compliance". In: *Sensor Applications, Experimentation, and Logistics: First International Conference, SENSAPPEAL 2009, Athens, Greece, September 25, 2009, Revised Selected Papers 1*. Springer. 2010, pp. 159–176
- Tony O'Donovan, Nicolas Tsiftes, Zhitao He, Thiemo Voigt, and Cormac J Sreenan. "Detailed diagnosis of performance anomalies in sensor-

nets". In: *Proceedings of the 6th Workshop on Hot Topics in Embedded Networked Sensors*. 2010, pp. 1–5

- Yian Qin, Zhitao He, and Thiemo Voigt. "Towards accurate and agile link quality estimation in wireless sensor networks". In: *2011 The 10th IFIP Annual Mediterranean Ad Hoc Networking Workshop*. IEEE. 2011, pp. 179–185
- Wolf-Bastian Pöttner et al. "WSN Evaluation in Industrial Environments First results and lessons learned". In: *2011 International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS)*. IEEE. 2011, pp. 1–8
- Zhitao He and Thiemo Voigt. "Zooming into radio events by bus snooping". In: *ACM SIGBED Review* 9.3 (2012), pp. 21–23
- Shahid Raza, Prasant Misra, Zhitao He, and Thiemo Voigt. "Bluetooth smart: An enabling technology for the Internet of Things". In: *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. IEEE. 2015, pp. 155–162
- John Kanwar, Niclas Finne, Nicolas Tsiftes, Joakim Eriksson, Thiemo Voigt, Zhitao He, Christer Åhlund, and Saguna Saguna. "Jamsense: Interference and jamming classification for low-power wireless networks". In: *2021 13th IFIP Wireless and Mobile Networking Conference (WMNC)*. IEEE. 2021, pp. 9–16

Contents

Part I:
Dissertation Summary

1. Introduction

When the Internet extends its digital tentacles deeper into our physical world, we are facing challenges to provide reliable and affordable wireless links to the vast amount of sensors, or “things”, that have become one of the fastest growing data sources. Unlike the human population, which is projected to peak later this century [2, 3], the number of "things" providing for our digital life will keep growing fast in the foreseeable future. However, just like a single software bug can spread across the Internet and cause a major disruption in our modern life, a security flaw arising from the Internet of Things (IoT) can potentially inflict severe damage.

The problem with IoT security is complicated by the limited computing and communication resources provisioned for each small device. Low cost and small size force the hardware designer to merge core sensing and communication functionality into a single wireless Microcontroller Unit (MCU) [1]; Diverse deployment locations and long battery replacement cycles further limit options for wireless connectivity to simple, autonomous network protocols based on low power radios. Furthermore, the human resources dedicated to monitoring and reporting security incidents among low-cost, fault-tolerant small devices are considerably lower than those dedicated to maintaining core Internet services. Any Internet outage or data leak becomes a major incident, so it is handled with urgency. Deciding how much data loss an IoT network should tolerate before raising the alarm is not as straightforward. Tools for diagnosing problems in these Low-power and Lossy Networks (LLNs) [4] tend to have limited accuracy, as so many devices are deployed in the wild and communicate in “the open air”, i.e., a radio medium shared with other wireless devices and networks.

With high-cost and high-accuracy tools out of the question, how can we then stress test the health of the radio links in an LLN, with a reasonable resource expenditure? In this dissertation, we strive to answer the question by repurposing the low power radio transceiver to an interference generator. We then go on to investigate a related security question: provided with such a low power radio, how much harm can a clever malicious actor cause to an LLN, by injection of illegitimate data? At last, we look at how to bootstrap an IoT device securely with a unique digital identity using just minimal resource consumption.

[1] A wireless MCU, or wireless SoC, is an MCU integrated with a radio transceiver.

1.1 Research Questions

In this section we will pose the key research questions, which will be answered subsquently in the dissertation.

1.1.1 Emulating a lossy radio link

A precondition for a wireless network to function reliably is good link quality between nodes. Any two nodes that can hear each other's radio signal can potentially form a link. Hence a self-organized, densely populated network tends to consist of a large set of links, albeit of various quality. Whereas good quality links add redundancy to a connected network graph, poor quality links can instead cause excessive retransmissions, which exacerbate contention for scarce bandwidth among low power radios and drain their batteries. A good quality link is characteristic of a sufficiently high signal-to-noise and interference ratio (SINR) relative to the radio's cochannel rejection:

$$SINR = \frac{S}{I+N} \geq -C$$

S, N, and I stand for received power, noise, and interference respectively; C stands for cochannel rejection. For ZigBee/IEEE 802.15.4 [5] and Bluetooth Low Energy (BLE) [6] radios, typical cochannel rejection ranges between -3 dB to -6 dB, i.e., the radio can correctly decode a frame when the received signal is 2x to 4x stronger than combined interference and noise on the current channel [7] [8]. We consider S and N to be stable over time, based on the assumption that, for a statically deployed IoT network made up of low power radios: factors such as transmission power, modulation and encoding are fixed; the propagation loss between two nodes is also fixed. Therefore, interference I is the key factor that temporarily turns a good link into a poor link, when a sudden increased level of interference leads to a drop of SINR below the threshold above. Unlike noise, interference has an event-driven character. When a coexisting wireless network suddenly generates a burst of messages, the radio transmissions present as external interference to an IoT network. The communication can also be affected by internal interference, e.g., when an end user triggers the transmission of a command whose radio signal ripples through a routing path. Predicting the exact moment an interfering device starts transmitting is hard. But the interference signal usually remains stable for a very brief period that corresponds to the air time of the transmitted packet. Therefore, only when two or more packets overlap in time do they interfere with each other.

For low power radios used in LLNs, the most common recovery mechanism for occasional, interference-caused packet loss is automatic retransmission of unacknowledged messages. The maximum number of retries and the backoff period between each retry thus have significant implication for network performance. A network simulator e.g. Cooja can simulate probabilistic link loss with coarse-grain timing [9]. But to understand actual packet loss in a given installation, and then to mitigate the loss by optimal configuration of protocol mechanisms such as automatic retransmission, we face the challenge of reliably recreating the condition when packet loss occurs. Whereas the raw performance of a radio link can be measured and optimized in an anechoic chamber using high-precision instrumentation, we need a much lighter weighted alternative to deal with the numerous lossy links in an open environment. *Can we emulate a lossy radio link with high precision using affordable hardware*?

1.1.2 Investigating risk of denial of service on low power radios

In the past two decades or so, major silicon vendors of single-chip low power radio transceivers and wireless MCUs embedded with such a transceiver, have upgraded their products by several generations. This has happened along with the standardization of ZigBee [10], Thread [11], and BLE [6]. Not only standardized functions on the PHY layer, such as spread spectrum symbol encoding, AES encryption, clear-channel assessment, have been consolidated on the silicon; frame processing functions which conceptually belong to the MAC layer, such as source address filtering and automatic ACK transmission, have also been integrated on the radio core to automate low-level protocol event handling, reducing the load on the main CPU. The recent emergence of dual-core MCU architectures [12], that comprise an application processor and a network processor dedicated to wireless communication, continues the trend of process automation of the radio transceiver.

The assumption that radio frames are always processed safely by the hard-coded on-chip state machine has seldom been questioned. In particular, an ZigBee/IEEE 802.15.4 radio receiver trusts blindly that detection of an Start-of-Frame Delimiter (SFD) is always followed by a legitimate PHY Header (PHR), which specifies the size of the incoming payload. Hardware-based address filtering and CRC checking ensure that only useful frames are stored and passed on to the next higher layer for further processing; corrupted or irrelevant frames are discarded automatically. However, no attempt is done to check whether the payload being decoded, one byte at a time, actually corresponds to a valid radio signal. The rationale is probably that successful detection of the preamble together with the SFD at the beginning of the frame hints at a high likelihood of a signal; the CRC checking at the end of the decoded payload removes any false positives. Therefore, extra filtering in-between is unnecessary; it would only create false negatives, i.e., mistaking a weak signal for noise and thus rejecting a valid frame.

This rationale, however, overlooks the issue that, for wireless IoT devices, bandwidth and energy consumed by the radio are resources too precious for wasteful reception of noise. Whereas occasional communication error can be tolerated and recovered from, the radio can be put under huge pressure to handle large amount of errors injected by a malicious party. For this reason, we pose the question: *Can the radio's automatic frame decoding inadvertently open the door to denial-of-service attacks?*

1.1.3 Assigning encryption keys to IoT devices

Low power radio transceivers have long supported optional transport security by means of hardware-accelerated symmetric encryption of messages. Hardware support of asymmetric encryption has been added in later generations of chips. The latest generation of wireless MCUs even includes protected memory areas for storage of encryption keys. On the other hand, many open-source embedded operating systems, such as Contiki-NG [13], include their own memory-optimized software ciphers. As the number of connected IoT devices increases, awareness of the need for data encryption also rises among vendors and users. The question is no longer whether data security justifies the extra cost of message encryption on an IoT network, but rather how to assign different keys for different purposes to the rapidly growing number of interconnected devices, in a secure and efficient manner. More specifically: *Can we provision each IoT device with a unique and easily verifiable digital identity, so that it can securely exchange information with any other device, and indeed any host on the Internet?*

1.2 Methods

All the work in my dissertation is based on experimental study on built artifacts. The artifacts are embedded software designed to carry out wireless communication for studying a hypothesis e.g a suspected effect on network performance caused by a certain type of radio interference. To isolate the effect of intentional interference from that of uncontrolled random noise and interference in the environment, we often first use RF cables to create low-noise links between a handful of radios. Only after we establish a good level of confidence about the cause and effect do we scale up the experiment in an open-air testbed, such as Flocklab [14], to collect data. Both the cabled experiments and the open-air experiments take many iterations of trial-and-error, to narrow down the parameter space to a small set of important variables with proper value ranges. Across the papers, the common performance metrics include packet reception rate, latency, and power consumption. For statistical reliability in the data measurement, we always repeat the same experiment multiple times. When an unexpected result arises, we conduct careful analysis before removing any outlier. In fact, it is what appears to be a small glitch in the data that leads to the discovery of the Droplet attack in Paper III.

Most of the embedded software developed in this work is built around the open-source Contiki OS that runs on Commercial Off The Shelf (COTS) hardware (or as a PC process). Because we are experimenting with low-level radio events, we often need to modify directly the radio and MAC drivers of Contiki. We use also a logic analyzer to capture radio events exported from certain MCU pins, and a spectrum analyzer to measure the power level of radio signals. For Paper V, we use Eclipse Californium [15], an open-source JAVA library for Constrained Application Protocol (CoAP), to run a test server that acts as a Certificate Authority.

1.3 Contributions

This dissertation contributes to the state of the art in the area of reliability and security of LLNs. We invent new methods to cause packet loss in radio links by intentional interference generated from small IoT devices equipped with low power radios. We then shed light on the PHY-layer security risks, posed by a malicious party in possession of the same kind of low-cost hardware. Finally, we come up with an cost-efficient method to bootstrap small devices with unique digital identities. We elaborate these core contributions from the five papers, that answer the research questions posed before.

Leveraging Intentional Radio Interference for Networking Tests

We repurpose the radio signal generated from a low power transceiver to emulate interference from external sources (Paper I). This allows us to reliably recreate the radio events that lead to loss of data packets. Experiments conducted with a controllable level of probabilistic packet loss are thus more time-efficient and reliable than those with only an unpredictable or coarsely estimated level of interference. Exploiting the built-in test modes on the transceiver for generating the needed signal saves hardware cost and reduces programming to a minimum, compared with other solutions. When combined with frame detection, a short burst of intentional interference can precisely take out a specific frame, leading to increased test coverage that helps us to uncover implementation flaws in networking protocols (Paper II). These tools drastically improve the accuracy and efficiency of tests on medium-to-large scale IoT networks.

Frame Injection DoS Attacks against IoT

We discover a new DoS attack against ZigBee/IEEE 802.15.4 radios, exploiting the automatic frame decoding mechanisms common in those transceivers. By repeated injections of falsified PHY headers, dubbed *droplets*, a malicious transmitter based on the same low power radio transceiver as its victims can achieve a similar effect as jamming (Paper II). All receivers who detect the attacker's signal, which encodes the minimum information of just one byte, are forced into decoding 127 bytes' worth of noise. Whereas an increased density of nodes in the network can potentially strengthen the radio links against jamming attacks, it can not fend off the Droplet attack due to the stealthy nature of the latter. The Droplet attack thus poses a serious threat to any wireless network based on the same PHY standard. An investigation on the header checking mechanism of Glossy, which makes it immune to the Droplet attack, leads us to the design of another DoS attack (Paper IV). Specifically crafted to pass Glossy's header checking, the Arpeggio attack emits falsified Glossy frames, which then flood the whole network far beyond the attacker's radio transmission range. Droplet and Arpeggio highlight the security risks for low power radios, which in spite of state-of-the-art encryption, can still be knocked offline by just a single or a handful malicious low-cost COTS radios.

Automatic Certificate Enrollment for IoT Devices

Taking the resource constraints on IoT devices into consideration, we design a lightweight but highly secure client for enrollment of digital certificates to these small devices (Paper V). To carry out certificate enrollment based on just a very small amount of pre-installed information, we reuse the EST protocol [16], a standard widely used to enroll certificate for Internet hosts. Originally designed to exchange request and response messages between a new host and a Certificate Authority over a secure HTTPs channel, our lightweight client can now transport the EST protocol over CoAPs, with minimal communication overhead. Preserving the EST protocol semantics, EST-over-CoAPs provides IoT devices with the same functionality and security level of a typical web host. With automated certificate enrollment, we take a big step towards extending the highly scalable Public Key Infrastructure (PKI) to IoT devices. Each small sensing device can now obtain a unique digital identity at the start of its life, which enables it to establish secure communication with any trusted party on the Internet and to feed data to various services.

1.4 Dissertation Structure

After this introduction, we continue the summary of the dissertation by presenting background and related work (Chapter 2). Chapter 3 summarizes the five peer-reviewed conference papers that constitute the core of my work. We finish Part I with conclusions and future work. Part II of the dissertation contains a reprint of the five papers.

2. Background and Related Work

In the chapter, we provide essential background and related work for the thesis. Each section is organized around a topic about PHY layer security or application layer security.

2.1 Coexistence of Radio Devices on the Unlicensed 2.4 GHz Frequency Band

The 2.4 GHz frequency band for industrial, scientific and medical (ISM) applications is dominated by various types of Short-Range Radioss (SRDs), such as WiFi and Bluetooth Classic devices. This license-free, around 80 MHz-wide band (2400-2483.5 MHz) is also increasingly inhabited by IoT devices such as ZigBee and BLE devices. How can so many heterogeneous radio technologies coexist in the same space without any centralized coordination? The primary reason is that they operate on a non-interference and non-protected basis, thanks to the technical standards set by International Telecommunication Union (ITU) and enforced by regional and national authorities [17–20]. Across the 10 ISM frequency bands commonly used across the world, ranging from 6 MHz to 240 GHz, the ITU technical standards set limits for various parameters e.g. occupied bandwidth, output power, and duty cycle. These PHY parameters are accompanied further by requirements on spectrum access techniques at the MAC layer. A typical technique is Listen Before Talk (LBT), a.k.a. clear channel assessment (CCA), where a transmission occurs only after the channel has been estimated to be idle. Natarajan et al. have studied cross-technology interference among IEEE 802.15.4, BLE and IEEE 802.11 on the 2.4 GHz ISM band, noting that both time and channel separation mechanisms can reduce packet error [21]. Figure 2.1 shows a spectrum snapshot of multiple signals on this band.

Looking specifically at the European requirements on SRDs operating on 2.4 GHz band [18, 19, 22], we identify two application types that typical IoT control and sensing tasks can map to, with different technical requirements. *Non-specific SRDs*, whose output power is capped at $10mW$ ($10dBm$) EIRP [1], have no additional requirements. This is a generic application type covering all kinds of low-power devices such as wireless keyboards and ZigBee sensors.

[1] EIRP (equivalent isotropic radiated power) is the total power fed into an ideal isotropic antenna, which radiates uniformly in all directions.

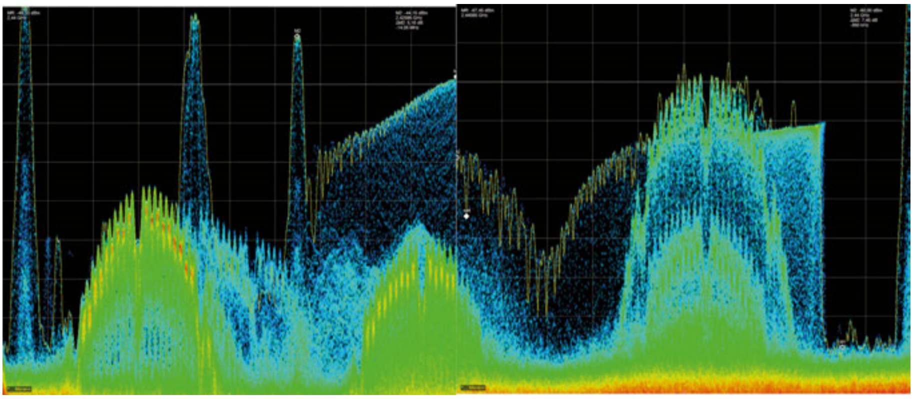
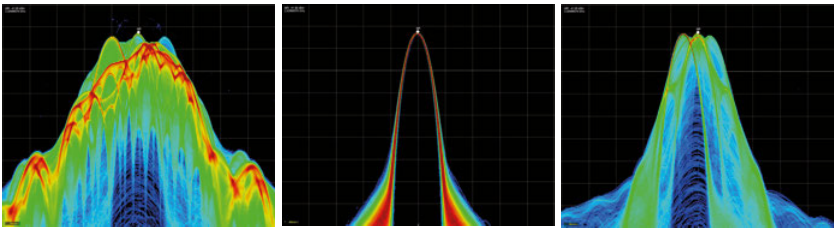


Figure 2.1. We use a a spectrum analyzer to capture a snapshot of coexistent signals in the frequency range [2400 MHz, 2480 MHz]. The 20 MHz-wide signals are from WiFi transmitters; the various narrow-band signals are from Bluetooth peripherals and wireless keyboards and mice communicating on a proprietary protocol.

Without requirements on modulation type, duty cycle, or any other interference mitigation techniques, these devices coexist peacefully, in principle, by simply capping their Tx power at 10mW. In reality, however, the industry such as IEEE802.15.4/ZigBee device vendors often choose to implement additional interference reduction techniques including CSMA/CA (a form of LBT), in order to optimize performance. On the other hand, *Wideband data transmission systems* e.g. WiFi and Bluetooth Classic devices have a higher output power limit at $100mW(20dBm)$. They are required to implement spectrum sharing mechanisms such as LBT and FHSS (frequency hopping spread spectrum). IoT sensors running ZigBee or BLE that already adopt spectrum sharing techniques can therefore potentially also fit into this category. They can increase output power up to $100mW$, if hardware cost and power consumption justify such an upgrade. Indeed, BLE and ZigBee chip vendors have designed wireless MCUs with integrated power amplifiers [23] or separate front-end modules [24] to allow a boost of output power to the WiFi level. The increasing number of IoT devices and their increased radio output power have recently led to concerns within ETSI regarding interference problems on the 2.4 GHz band [25]. Hence our work on understanding and recreating cross-technology radio interference on the 2.4 GHz band, dated back in early 2010s, is still highly relevant today.

2.2 Signal Waveforms of 2.4 GHz Low-power Radios

A multi-standard low-power radio can generate a number of different signals depending on the chosen modulation standard. Additional test signals are often accessible, too. We show a few signal spectra of the nRF52840 System-on-Chip, captured on a spectrum analyzer, in Figure 2.2.



(a) IEEE 802.15.4 packets, a 4 MHz-wide signal

(b) Unmodulated carrier, a continuous-time monotone test signal

(c) Fixed-channel BLE packets, a 2 MHz-wide signal, generated under Bluetooth Direct Test Mode

Figure 2.2. Signal spectra generated by different modulation modes of the Nordic-Semiconductor nRF52840 featuring an on-chip ZigBee/BLE radio transceiver. The retail price of the chip is $8, which drops to $5 in larger volume.

Signals such as the unmodulated carrier and the fixed-channel BLE packets are intended for quality control tests during hardware production. There is no restriction, however, on the firmware developer to leverage these test signals for more advanced communication tests. More generally, the chip implements only the bottom PHY layer of a standard communication stack such as ZigBee or BLE, leaving a large part of the next-higher MAC layer to be implemented as firmware, on the Flash memory shared with the operating system and the application. This architectural design saves hardware cost, and allows for the flexibility of plugging in standard or proprietary MACs as separate firmware libraries. On the flip side, giving the firmware developer direct access to the PHY layer increases the risk of misuse, both intentional and unintentional, of the radio. In this dissertation, we have exploited the full access to the radio PHY, to carry out both protocol testing and cyber attacks.

An interesting comparison can be made against commercial WiFi transceivers, which operate on the same unlicensed 2.4GHz band. WiFi chips must support a larger set of modulation and encoding schemes, together with advanced radio control features, specified under the IEEE 802.11 standard. The software complexity of the WiFi PHY and MAC, and the need for interoperability among a large number of device vendors, lead chip manufacturers to store the firmware in dedicated Read-Only Memory (ROM). As a result, the underlying PHY functionality is sealed from accidental misuse by the OS. This practice nonetheless does not completely stop crafty reverse engineering and firmware patching from gaining access to the PHY of some WiFi chips. Security researchers have been able to sniff raw WiFi data in the air and to generate intentional interference [26] [27] [28].

2.3 Signal Coverage Estimation Based on Path Loss

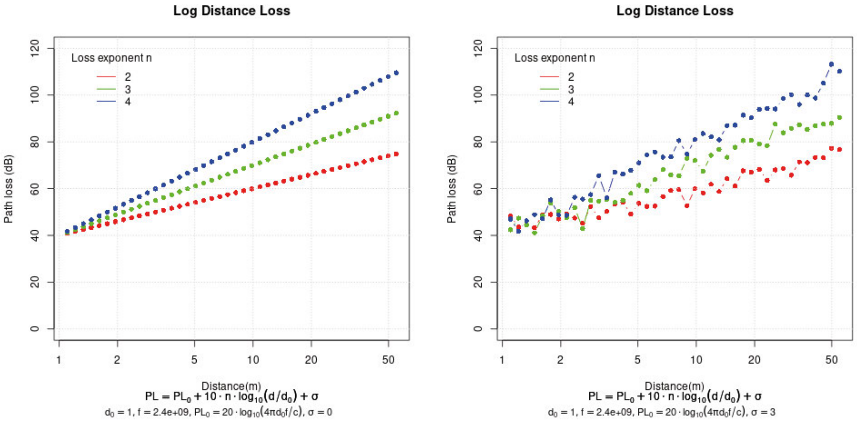
Because a radio signal radiates in all directions, it loses strength as it travels due to decreasing area power density. A radio receiver at distance thus picks up from its antenna only a tiny fraction of the transmitter's radiated power. Planning the deployment of an indoor wireless network involves calculations of signal coverage based on path loss. In an indoor environment, such as home and office, the basic, distance-dependent propagation loss described above is combined with loss caused by the environment: reflection, diffraction, scattering, etc [29]. The combined effect of these factors, as often observed, is an environment-specific, near-constant, rate of signal attenuation over distance, plus a degree of variation caused by channel fading. The *log-distance path loss model* captures the rate of attenuation in the form of loss exponent, and the variation component as a zero-mean Gaussian noise [29]:

$$PL = PL_0 + 10n\log_{10}\left(\frac{d}{d_0}\right) + X_g \tag{2.1}$$

Where n is the loss exponent, X_g is zero-mean Gaussian noise, and PL_0 is the free-space path loss at reference distance d_0:

$$PL_0 = 20\log_{10}\left(\frac{4\pi d_0 f}{c}\right) \tag{2.2}$$

When traveling in free space, a radio signal attenuates at a rate quadratically proportional to distance, i.e., $n = 2$. In a specific indoor environment, the loss exponent depends heavily on the spacial structure of the floorplan, according to an ITU recommendation on radio LAN planning [30]. A grocery store featuring long and narrow corridors has a tunnel effect reinforcing the radio signals, resulting in path loss lower than free-space loss, i.e., $n < 2$; Signal propagation inside a large wearhouse is dominated by free-space loss, thus $n \approx 2$; On an office floor with small, separate rooms, interior walls create many non-line-of-sight propagation paths, leading to path loss as high as $n = 4$ [30]. For illustration of the influence of loss exponent on range, we plot the log-distance path loss for a 2.4 GHz signal (without noise) in Fig. 2.3a. Considering that our interested low-power radios have a typical range of 10 to 50 meters indoors, we set a small $d_0 = 1m$. The three curves corresponds to loss exponent $n = 2,3,4$. When planning a deployment, to ensure good connectivity, extra allowance in the link budget needs to be allocated to counter the detrimental effect of random noise. The level of noise is however highly dependent on the environment. Furthermore, in the same environment, non-line-of-sight paths have a significantly larger degree of randomness than line-of-sight paths. For example, in an industrial environment, random noise in non-LoS paths has standard deviation between 6.3 to 9.0 dB [30] [31]. In an early experimental study on link quality of an indoor wireless sensor network, Zhao et al. note the existence of a large "grey area" on the edge of a transmitter's Tx range, where packet reception becomes highly unstable [32]. Fig. 2.3b illustrates the effect of channel fading on path loss, caused by e.g. multipath and shawdowing, by plugging in a moderate amount of Gaussian noise $X_g \sim N(0,3)(dB)$ to the log distance model.



(a) Log-distance path loss without noise

(b) Log-distance path loss with Gaussian noise

Figure 2.3. The log-distance path loss model can be used to predict how far in distance a signal can travel. A 2.4 GHz signal has a loss of $\sim 40dB$ at $1m$, which then increases with distance. A 10 dBm signal transmitted from a low power radio can sustain a estimated path loss of 110 dB and still be detected by a receiver with -100 dBm sensitivity; but the practical need to accomodate random channel fading means the link budget should be 110 dB for reliable communication.

Despite best efforts in deployment planning, real path loss in any specific environment always deviate from the predictions of these simple mathematical models [33]. Moving obstacles and external interference further compound the problem of range estimation. Paper I & II in this dissertation address the need for pragmatic tools to facillitate testing of link quality in a deployed network.

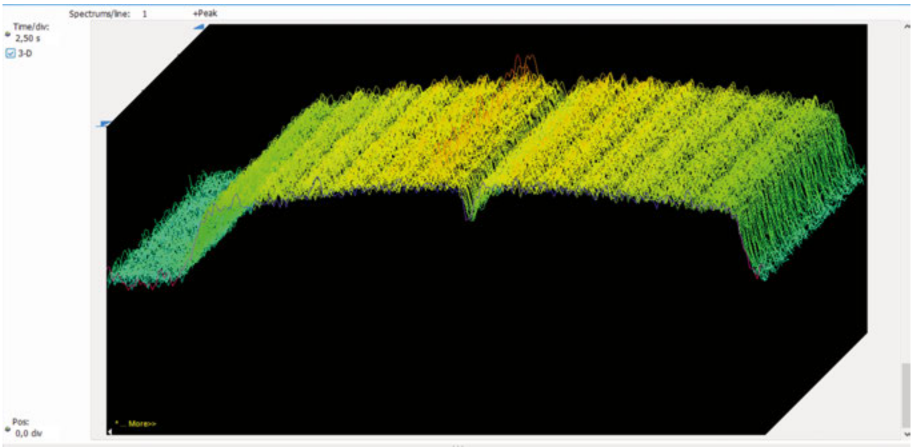
2.4 Reception Errors Caused by Interference

Whether an interfering signal corrupts a decoded symbol, which in turn leads to a packet error, depends primarily on two factors: 1. how much interference is picked up by the receiver; 2 the receiver's filtering capability to select the wanted signal in presence of interference.

IEEE 802.15.4 and BLE receiver chips have good Rx selectivity under interference on other channels. They can suppress relatively strong interference, typically 30 dB above the wanted signal, on a non-overlapping, adjacent channel [7] [8]. A large proportion of the received interference is filtered out before entering the demodulator.

The main cause of packet error inside the communication range is thus cochannel interference, i.e., unwanted signal overlapping with the wanted signal in frequency. Both the wanted signal and the cochannel interference are amplified by the automatic gain control (AGC) at the receiver circuitry. A receiver has typically a negative cochannel rejection of -3 to -6 dB. This means cochannel interference 3 to 6 dB *weaker* than the wanted signal would be sufficient to corrupt the received packet.

A wideband signal e.g. WiFi can interfere with multiple IEEE 802.15.4 or BLE channels simultaneously; on a specific narrowband channel, however, WiFi interference is usually not perceived to be more powerful than narrowband cochannel interference, because only a fraction of its total received power enters the narrowband receiver. Fig. 2.4 shows a narrowband BLE signal being interfered by a WiFi signal generated from a Raspberry Pi using the Jamlab-NG utility [27].



Spectrums/line: 1

Time/div: 2,50 s

☑ 3-D

Pos: 0,0 div

Figure 2.4. We use a Rapsberry Zero W to generate a 20-MHz wide, OFDM modulated WiFi signal that interferes with a 2-MHz BLE signal at the center of the former's spectrum.

Because interference also suffers from path loss, its effect on different communication links within its Tx range depends on the its relative power compared with different wanted signals perceived at a specific receiver: it can block a few transmitters completely, shorten the effective Tx ranges of others by different degrees, and yet incur no damage at all to some others. This makes it hard for a single interferer to completely disconnect a sprawled, multihop wirleless IoT network; but it also makes detection a complex task, as the received signal strength varies greatly across different locations. Boano et al. developed Jamlab, an infrastructure comprising dedicated IEEE 802.15.4-based interferer nodes that overlaps physically with a sensor network testbed, in order to systematically study network-wide performance under interference of different time patterns and levels of severity [34]. JamLab-NG, a derived work of JamLab, is capable of generating dummpy 802.11b/g packets in very short intervals on the 2.4GHz band for the same purpose [27]. Wu et al. used Software Defined Radios (SDRs) to perform a controlled experiment on an IEEE 802.15.4 link, and observed distinct chip error patterns under interference-free and interference conditions [35].

Because the receiver is capable of rejecting cochannel interference below a power threshold relative to the power of the wanted signal, it can therefore tolerate internal interference concurrently sent from fellow nodes belonging to the same network, avoiding packet collisions. The *power capture effect* described above [36–38] is one of the two mechanisms that underpins the Glossy fast flooding protocol [39], which we exploit in a DoS attack in Paper IV. Fig. 2.5 shows IEEE 802.15.4 data packets transmitted on eight channels overcoming cochannel interference from monotone jammers at respective center frequencies, thanks to the 6 dB power advantage.

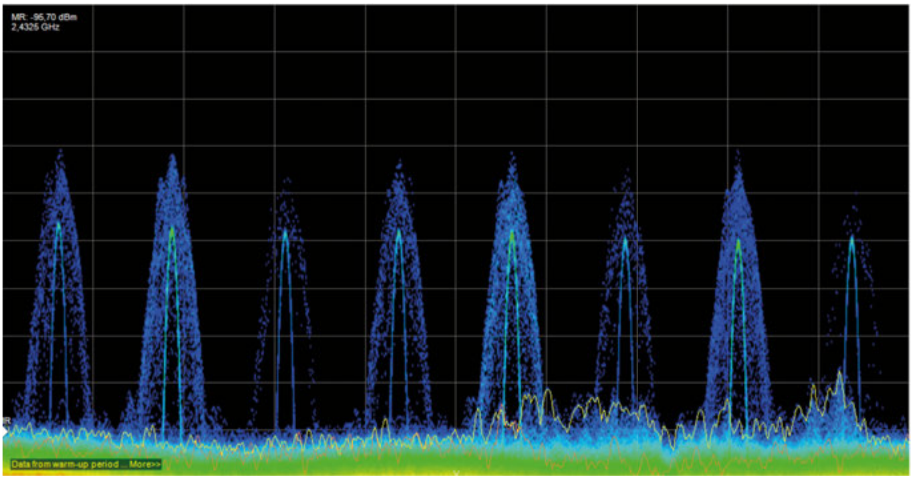


Figure 2.5. IEEE 802.15.4 communicate over eight interfered channels without error, because the power of the monotone jamming signals (green peaks) are slightly lower than the wanted signal (blue peaks).

2.5 IEEE 802.15.4 Frame Detection and the Droplet Header Injection Attack

An IEEE 802.15.4 radio frame on the PHY layer (a.k.a. PPDU) consists of a synchronization header, followed by a PHY header, and then a payload, as shown in Fig. 2.6.

When a powered-up radio is not actively transmitting or receiving data, it is constantly searching for incoming frames on the configured radio channel. Specifically, the receiver tries to map the stream of demodulated and

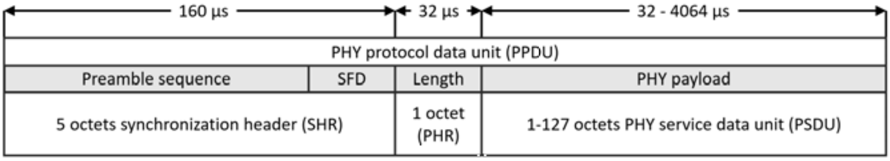
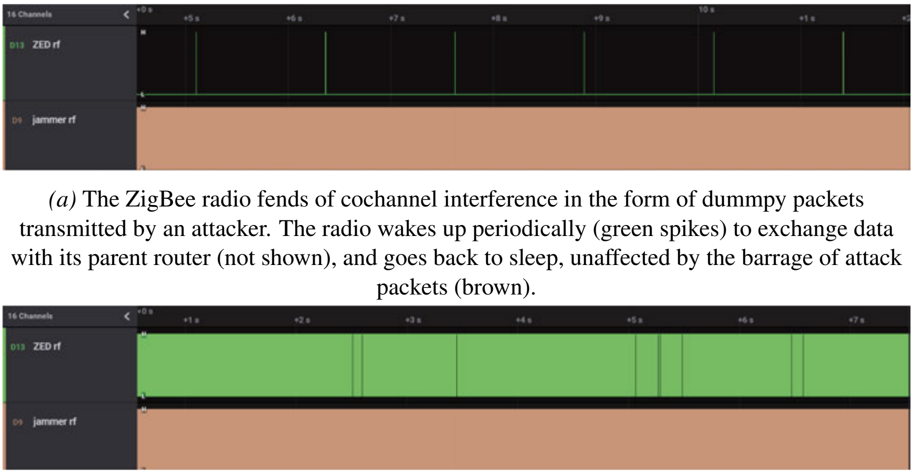

160 µs
32 µs
32 - 4064 µs
PHY protocol data unit (PPDU)
Preamble sequence
SFD
Length
PHY payload
5 octets synchronization header (SHR)
1 octet (PHR)
1-127 octets PHY service data unit (PSDU)

Figure 2.6. IEEE 802.15.4 frame format

decoded digital symbols with those defined in a standard Synchronization Header (SHR). The preamble sequence consists of repeated zero symbols to help the demodulator adjust to the transmitter's center frequency and establish time boundaries between symbols; the SFD is a fixed value octet that helps to establish boundaries between each incoming byte thereafter. The PHR encodes the length of the PHY payload, ranged btweeen 1 to 127 bytes. Because IEEE 802.15.4 fully specifies the Orthogonal Quadrature Phase Shift Keying (O-QPSK), Direct Sequence Spread Spectrum (DSSS) PHY, interoperation between different chips is expected. There are even SDR implementations [1] [40] [41]. In reality, however, most network deployments comprise homogeneous devices from the same vendor. Apart from the usual single ownership of an IoT network, a technical reason is that device vendors want to optimize performance by selecting a MAC protocol and higher-layer components from a plethora of choices, either standardized or proprietary. Even the IEEE 802.15.4 specification alone provides various MAC-layer options. Unslotted Carrier Sensing Multiple Access (CSMA), slotted CSMA, Time Synchronized Channel Hopping (TSCH), etc., are incompatible with each other. The 2.4 GHz PHY is therefore the common denominator of various IEEE 802.15.4-based radio devices, including ZigBee, Thread [11], IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) [42], etc. A vulnerability on the PHY layer affects all those devices.

We discovered one such vulneralbility on the IEEE 802.15.4 PHY in Paper III. An attacker can send 6 byte-long frames to spoof the SHR and PHR, which triggers frame detection and decoding in all listening radios in range, resulting in denial-of-service of those affected nodes for a period equivalent to a maximum size PPDU ($4256\mu s$). At the time of discovery, the *Droplet attack* was shown to be effective against ContikiMAC, an open-source but non-standard CSMA-based MAC protocol. 10 years later, we were able to reimplement the attack on a new radio chip and successfully cause DoS in a commercial ZigBee stack (Fig. 2.7).

Bellardo et al. identify a vuneralbility in the 802.11 virtual carrier sensing mechanism, which allows an attacker to reserve the channel for $32ms$ by sending a short request-to-send (RTS) packet [43]. Conceptually, this attack is very similar to our Droplet attack. An RTS with a spoofed duration, in this



(a) The ZigBee radio fends of cochannel interference in the form of dummpy packets transmitted by an attacker. The radio wakes up periodically (green spikes) to exchange data with its parent router (not shown), and goes back to sleep, unaffected by the barrage of attack packets (brown).

(b) The ZigBee radio is deprived of both sleep and bandwidth by a Droplot attacker.

Figure 2.7. A normally low-power ZigBee End Device (ZED) under cochannel interference and Droplet attack. We use a logic analyzer to capture the on/off events of the two nRF52840 radios.

case not for the control frame itself but a subsequent data frame, strikes off an unproportionally large slice of usable channel time from all listening radios in range. Unlike the Droplet attack, the 802.11 attack does not trigger active decoding on its vitims, thus has no battery draining effect.

Krentz et al. design a specific mitigation mechansim against droplet injections, by replacing the standard 802.15.4 MAC header with a custom one and performing on-the-fly check on a one-time password (OTP) [44]. The OTP is generated by AES encryption of a secret value formed by combining a predistributed network-wide key, a group session key of the sender, the destination address, and a frame counter. As soon as the OTP field of the MAC header is received, the receiver can compare it with a locally computed value; if the check fails, the radio discards the incoming packet and terminates the ongoing reception, in the best case with a short delay of just $250\mu s$. Krentz et al. later also developed defenses againt a broader range of denial-of-sleep attacks against ContikiMAC [45] and the IEEE 802.15.4 CSL MAC [46].

2.6 The Glossy Flooding Protocol and Related Denial-of-Service Attacks

For common sensing and control tasks in the IoT, the dominant traffic pattern is end-to-end unicast between a single low-power end node and the gateway node. The incentive to optimize the latency and reliability of such traffic leads to design of routing protocols over tree-like multihop topologies, such as the Collection Tree Protocol (CTP) [47, 48] and IPv6 Routing Protocol for Low-

Power and Lossy Networks (RPL) [49]. On the other hand, there is a less frequent yet important need for one-to-many communication, such as routing information propagation and firmware update, which requires a message to be disseminated to all nodes in the wireless network in a reliable, albeit delay-tolerant manner. Obviously, this traffic pattern maps poorly to point-to-point routing. Flooding protocols in WSNs therefore have been designed to specifically optimize one-to-many communication. Notable examples are Trickle [50, 51] and Flash [52, 53]. The invention of the Glossy rapid flooding protocol by Ferrari et al. [54] overthrew the previous assumption that flooding needs to be rate controlled, lest the network becomes saturated with destructive interference among the participating nodes. By leveraging precisely time-synchronized transmissions, Glossy nodes immediately re-broadcast a received message after incrementing its relay counter, resulting in quick dissemination across multiple hops in a matter of just tens of ms.

Because Glossy flooding is fast and reliable, expanding it to carry unicast traffic becomes technically viable. Using Glossy flooding as the underlying transport mechanism, the Low-Power Wireless Bus (LWB) [55] uses a centrally managed, timeslotted schedule to give any node a fair share of the channel for sending to any other node(s). Rapid flooding provides the illusion of a single-hop, low-latency link, hence the notion of *wireless bus*. The Chaos protocol by Landsiedel et al. leverages synchronous transmissions to achieve rapid data aggregation in large-scale low-power wireless networks [56].

The authors of Glossy originally attributed its seemingly collision-free flooding primarily to *constructive interference*, whereby concurrent transmissions amplify, rather than destroy, the original signal, thanks to very accurate time synchronization. Liao et al. however disputed this claim, by pointing out that carrier frequency offset between concurrent transmitters creates a beating effect similar to deep fading. Consequently, even two perfectly time-synchronized IEEE 802.15.4 frames still have a high likelihood of having portions of their symbols destructively interfering each other. The reliability of Glossy should therefore be attributed to the capture effect and the error correction capability of the DSSS coding of IEEE 802.15.4. In a comprehensive survey on synchronous transmissions in low-power wireless conducted by Zimmerling et al. [57], the authors acknowledge that the term constructive interference is technically incorrect, but reaffirm that synchronous transmissions do appear to provide robust transport for the link layer.

Nonetheless, our main interest is not the efficiency, but rather the security, of Glossy. Can a malicious program disrupt Glossy flooding, by eavesdropping and transmitting radio frames using the same hardware? Hewage et al. were the first to challenge Glossy with three specifically crafted DoS attacks, and found that one of them, the relay counter modification attack, renders the nodes to lose synchronization [58]. Our Arpeggio attack in Paper IV directly injects bogus Glossy packets to hijack the flooding mechanism, without any need for time synchronization or eavesdropping. It highlights the need for

Glossy to perform header checking and early termination of futile frame reception. We believe leveraging header encryption by Krentz et al. [44] will provide effective mitigation. Lockie et al. have bolstered Atomic, another synchronous flooding protocol [59], with message confidentiality and authentication [60]. Encrypting messages, however, does not prevent header or frame injection DoS attacks such as Droplet and Arpeggio. Interestingly, the authors have reported that occasionally a corrupted frame size leads to schedule overrun and desynchronization, thus have been forced to set a maximum frame size in order to terminate reception of large frames.

2.7 The CoAPs IoT Protocol Stack

Palattella et al. proposed an IoT communication architecture that stacked up a set of standardized protocols [61]. Compared with previous architectural designs for low power WSNs e.g. Z-Wave and ZigBee that prioritize optimization of key performance metrics for the wireless LAN, the new IoT stack adds the explicit goal of turning constrained radio devices into standalone Internet hosts. These devices can be seamlessly integrated with the Internet, thus enjoy scalable connectivity and provide a familiar end-user experience. Specifically, 6LoWPAN [42] enhances IEEE 802.15.4-based devices with IPv6 addressing while minimizing overhead; RPL [49] provides efficient routing in a multihop low power WLAN; CoAP [62] preserves HTTP-style client-server semantics and provides end-to-end reliability that UDP lacks. The CoAP specification includes support of communication security in the form of Datagram Transport Layer Security (DTLS) [63] over UDP. With this, secure CoAP (CoAPs) protects application data with confidentiality and integrity. Fig. 2.8 shows the CoAPs stack we use in Paper V.

A recent standard, Object Security for Constrained RESTful Environments (OSCORE), further provides protection on the upper sublayer of CoAP, by means of symmetric key-based encryption of CoAP request/response messages [64]. As a result, OSCORE can operate with or without lower-layer security provided by e.g. DTLS.

The Open Mobile Alliance has developed the Lightweight M2M (LwM2M) application layer protocol for primarily resource constrained IoT devices [65]. LwM2M specifies an extensible, hierarchical resource model that organizes information under a number of objects. Messaging in LwM2M is inspired by the RESTful design of CoAP, and supports a range of transport mechanisms, including both CoAPs and OSCORE [66].

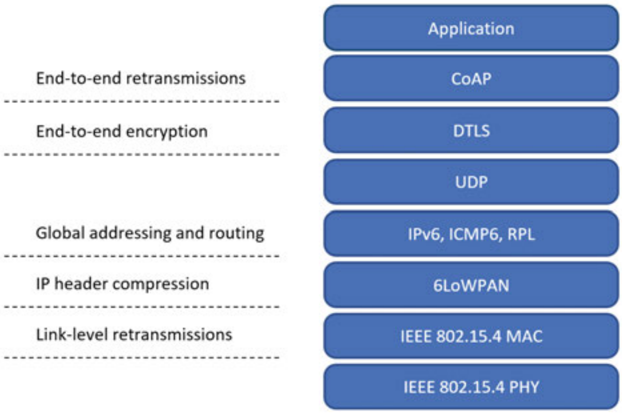


Figure 2.8. The secure CoAP (CoAPs) IoT stack provides a low power device with secure communication with any Internet service. We use this stack to perform digital certificates enrollment in Paper V.

2.8 Public Key Infrastructure for IoT

The vision to extend the Internet to a wide range of small devices to enable a host of new applications has gained traction across many industries. On the other hand, the risk that comes with granting direct Internet access to autonomous, potentially insecure IoT devices also pushes regulators and standard design organizations to establish provisions that require the use of best-practice cryptography in IoT. Some notable regulatory and standardization work in EU are the updated Radio Equipment Directive (RED) [67] and the ETSI standard on baseline cybersecurity requirements for consumer IoT [68]. Particularly, the increasing diversity and complexity of emerging IoT services underline the pressing need for a scalable means to manage encryption keys based on device identity. The ETSI standard includes a provision strongly encouraging the use of open, peer-reviewed standards for key management [68]. Adoption of the PKI, whereby trusts between hosts are established by verification of their digital certificates, is obviously a superior solution compared with proprietary schemes. Ting et al. enable a sensor node to use identify-based cryptography to send messages to an Internet host by offloading certificate verification to an offline stage [69]. Raza et al. show the feasibility of running CoAP over DTLS using X.509 certificates for hand shaking [70].

Our work in Paper V was the first to automate certificate enrollment for IoT devices, by adapting the EST enrollment protocol [16] over the CoAPs stack. This work later evolved into the IETF EST-coaps standard [71]. The LwM2M specification defines five security modes about what credentials are used, of which *Mode 4* exclusively reuses an earlier draft of the EST-coaps standard [66]. Since then, Forsby et al. have developed lightweight X.509

certificates using CBOR [72], an encoding more compact than ASN.1, thus reducing the amount of data transferred during enrollment [73]. Höglund et al. have developed LICE, an new variant of EST-coaps that leverages OSCORE and EDHOC [74] to further reduce protocol overhead [75]. The authors also add certificate revocation, an important, previously missing functionality for certificate lifecycle management in PKI for IoT [76].

3. Summary of Papers

3.1 Paper I

Carlo Alberto Boano, Zhitao He, Yafei Li, Thiemo Voigt, Marco Zuniga, and Andreas Willig. "Controllable radio interference for experimental and testing purposes in wireless sensor networks". In: *2009 IEEE 34th Conference on Local Computer Networks*. IEEE. 2009, pp. 865–872. DOI: `10.1109/LCN.2009.5355013`

Summary

The goal of the paper is finding a low cost and precise method to generate radio interference for testing WSNs. Several methods using different hardware and software are tested. Packet storms generated by WiFi and IEEE 802.15.4 radios are low cost, but imprecise. Software-defined radios can generate precise waveforms, but are too costly. We discover that the CC2420 radio chip used by wireless sensor nodes themselves is capable of generating two highly stable interference signals. By putting the radio under special test modes and controlling precisely the Tx power and on-off timing, we can generate interference patterns useful for injecting packet loss into networking experiments.

Reflections

The description of the two Tx test modes in the CC2420 datasheet was quite succinct. My experience in circuit design helped me to fill the gap between these fringe features and their intended use cases. The test modes are probably used by device manufacturers to conduct quality control on raw radio performance. For instance, precise Tx power level can be measured by an RF power meter when the device is transmitting in the unmodulated carrier mode. On the other hand, a measure of a receiver's bit error rate can be reliably attained by feeding the device with a bit sequence generated with the modulated spectrum mode. Conducting these measurements with the normal packet mode would be more time consuming and less accurate. I then reasoned that applying the test modes for interference generation would save time and yield higher quality data for WSN experiments.

The modulated spectrum mode later led to the accidental discovery of the Droplet effects in Paper III.

A skeptical opinion about the novelty of using the CC2420 test modes was that exploiting the uncommon feature amounts to just a clever hack.

With the benefit of hindsight, I can confidently claim that this rare feature 15 years back has now become a common feature, not just within the lineage of the TI Chipcon radio family, but also widely available across competitor chip vendors. In my current employment in the industry, I generate controlled interference using Nordic Semiconductor's nRF52840, a wireless MCU with over 10x more CPU power and memory than the MSP1611 on Tmote Sky.

My former colleague Carlos Penichet later came up the idea of using the unmodulated carrier Tx mode as the excitation signal of battery-free backscatters [77] [78]. The publication of his series of work in reputed conferences is additional evidence of the novelty of such a "clever hack".

My Contribution

I discovered the two CC2420 test modes for continuous transmissions when I plowed through the datasheet in search of advanced features. I then built a Contiki-based interference transmitter by enabling the test modes. Placing another Tmote Sky running an RSSI sampler program nearby, I showed a stable, elevated noise level over successive samples, a feature so far elusive from other low-to-medium cost means. This paved the way for Carlo to further develop a parameterized interference generator using just the low-cost CC2420. My contribution to the writing concentrated on the usage of the test modes for interference generation, including the code examples, in Section 4.2.

3.2 Paper II

Zhitao He and Thiemo Voigt. "Precise packet loss pattern generation by intentional interference". In: *2011 International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS)*. IEEE. 2011, pp. 1–6. DOI: 10.1109/DCOSS.2011.5982225

Summary

Using a single CC2420 radio, we develop a technique to shoot down detected radio packets mid-air by reusing the intentional interference in Paper I. Fast and reliable detection of any IEEE 802.15.4 radio packet is enabled by capturing the earliest state change in the interferer's radio, i.e., the detection of the Start-of-Frame delimiter (SFD) header. The interferer then quickly switches from Rx to Tx, to transmit a short jamming pulse to corrupt the payload of the packet. An application-specific decision function can be inserted between detection and transmission, so that the interferer reacts only to certain detected packets. Adjusting the decision function thus allows us to generate arbitrary packet loss patterns out of a perfect link, such as emulating an asymmetric link with distinct PRRs in forward and reverse directions. Manipulating an asymmetric link leads to a surprise discovery of two bugs in the automatic link-layer restransmission mechanism of Contiki OS. Our evaluation shows that this tool can help the network stack developer fix misconfigurations and implementation errors.

Reflections

This work is derived from the low-cost interference generator of Paper I, but takes an interesting turn. Rather than reconstructing a major *cause* of packet loss by adding interference, here we aim at emulating the *effect* of packet loss by direct interception. Carlo Boano, my coauthor in the previous paper, goes on to develop a full infrastructure of interferer nodes that emulate real-world interference sources (JamLab [79]). JamLab answers the question about network robustness under a typical scenario, as well as hypothetical questions under variants of the typical scenario. Here we answer similar questions regarding network robustness, albeit gearing toward unusually stressed conditions that the network is designed to survive. This work serves therefore a complementary function to Paper I and Jamlab.

My Contribution

I designed and implemented the reactive jammer on the Contiki OS-based TelosB platform. I also conducted the network experiments and performed the data analysis. I collaborated with my supervisor Thiemo on the write-up, me writing the original text and Thiemo refining it.

3.3 Paper III

Zhitao He and Thiemo Voigt. “Droplet: a new denial-of-service attack on low power wireless sensor networks”. In: *2013 IEEE 10th International Conference on Mobile Ad-Hoc and Sensor Systems (MASS)*. IEEE. 2013, pp. 542–550. DOI: 10.1109/MASS.2013.18

Summary

This paper reports the design of a novel DoS attack at IEEE 802.15.4 radios. The attack has a range remarkably longer than jamming. An accidental discovery during a jamming test exposes a vulnerability in the radio’s frame decoding procedure. Decoding the size of an incoming frame from the unencrypted

LEN header locks the receiver into a continuous period of payload decoding, during which it is deaf to other transmissions. An attacker thus can emit falsified frames including a LEN header but no payload, termed here as *droplets*, to trick receivers in range into decoding of non-existent data frames. Against sleepy radios running on a low duty cycle, the Droplet attack has a low hit rate, thanks to the narrow awake time window of its targets. We introduce Drizzle, a high-intensity variant of Droplet, that packs multiple Droplet headers into a seamless byte sequence. Drizzle is shown to be highly effective against the sleepy ContikiMAC.

Reflections

Ten years after the publication of this work, I can say that the Droplet attack remains highly effective and hard to defend. In my current employment in the security industry, I have been able to reimplement the Droplet attack on a recent chip and demonstrate complete network disruption to a ZigBee network running on a commercial stack. I have also developed a time-slotted and channel-hopping version of Droplet, which is capable of launching power-efficient DoS attacks on a TSCH network.

Because the vulnerability lies in hardware-automated frame decoding, it is possible to detect and mitigate an attack by modifying the frame reception state machine in the radio.

My Contribution

I discovered by accident the small but long-distance damage caused by normal data frames in an experiment. Investigation of the radio's frame decoding mechanism then led me to the design and implementation of the Droplet attack, which amplifies the damage. I conducted the quantitative study, which involved a number of hardware-based experiments and subsequent data analysis. I wrote the original text, which was refined by Thiemo's comments and edits.

3.4 Paper IV

Zhitao He, Kasun Hewage, and Thiemo Voigt. “Arpeggio: A penetration attack on glossy networks”. In: *2016 13th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*. IEEE. 2016, pp. 1–9. DOI: `10.1109/SAHCN.2016.7732971`

Summary

This work extends the previous one, by applying a packet injection DoS attack against the highly robust flooding protocol Glossy. We first investigate the reasons why our initial and second attempts of header injection failed. We then come up with a new attack named Arpeggio that, instead of injecting falsified frame headers, injects falsified, minimum-size frames. When such frames are embedded in a continuous Drizzle byte stream, Glossy's rapid flooding mechanism becomes hijacked; the subsequent flooding overwhelms the whole network with the attack frames, paralyzing normal data traffic.

Reflections

In hindsight, this work can been viewed as a rather straightforward adaptation of the Droplet attack for Glossy-based networks. The implementation is fairly trivial. What gives weight to the work is the identification and analysis of the problem itself. In my previous papers, the problem begins as a general idea, then becomes refined as the technical solution takes shape. Here I am directly challenged with a concrete problem, reported by my colleague Kasun, who reuses the Droplet attack but is unable to disrupt Glossy. Not knowing the Glossy internals so well as Kasun does, I conduct my investigation in gingerly steps, genuinely open to the possibility of failure. That I not only find an effective attack based on Droplet, but also surprisingly exploits a special property of Glossy to extend the damage range to the whole network, is a thrilling experience of discovery.

Using a full-duty Drizzle byte stream to carry the attack frames is far from being energy-optimal. Considering the high periodicity of Glossy floods, a time based, intermittent byte stream of attack frames can potentially achieve the same damage severity with much lower power consumption.

The paper stops at the evaluation of the effect of the Arpeggio attack, without further discussion of possible defenses. A natural question would be: could encryption of Glossy frames prevent or mitigate the attack? I think it could be both challenging and interesting to attempt encryption on Glossy frames while preserving sensitive timing: 1. Immediate termination of the ongoing reception of an illegal frame implies header decryption using a stream cipher, which is harder to integrate into the time-sensitive radio driver due to the need for state maintenance and the lack of hardware accelerator support; 2. The per-hop increments of the Glossy flooding counter would require repeated decryption and re-encryption of the frame at each step of flooding, squeezing the time error margin.

My Contribution

After verification of the failed Droplet/Drizzle attack against Glossy by repeating Kasun's test, I conducted code analysis of Glossy's highly innovative but complex radio driver. Identification of the frame filtering mechanism and the increasing idle listening time along downstream nodes eventually led to the design of the Arpeggio attack. Convinced with the initial results from my desktop testbed using Kasun's Glossy/LWB implementation, I launched large-scale experiments on the Flocklab testbed and collected the data, again taking many useful tips from Kasun. As first author I was responsible for a large part of the writing, except Sec. 2.1 and 5.2, which are Glossy/LWB background and timing configuration written by Kasun, who also contributed some citations in Related Work. Thiemo contributed dozens of comments and edits during the process.

3.5 Paper V

Zhitao He, Martin Furuhed, and Shahid Raza. "Indraj: digital certificate enrollment for battery-powered wireless devices". In: *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*. ACM. 2019, pp. 117–127. DOI: `10.1145/3317549.3323408`

Summary

This work facilitates the expansion of the Internet's public key infrastructure (PKI) to the sphere of IoT, with automatic certificate enrollment for small devices. By just adding an enrollment client service on the device, the security level and server-side infrastructure of Internet PKI are retained. The gist of the design is porting a widely used certificate enrollment protocol, Enrollment over Secure Transport (EST), from a HTTP/TLS/TCP protocol stack to a alternative, lightweight stack for IoT devices.

The main challenges are keeping the on-device EST client slim and power-efficient. To this end, we implement just an essential subset of the EST protocol, supported by a number of standard-compliant message codecs; we implement a certificate store on the on-chip flash memory. EST messages are transported over CoAP, which together with DTLS provide end-to-end transport security but add minimal overhead. After investigation on trade-offs between latency and power consumption, our evaluation concludes that a new device programmed with a preshared key can boot up and finish enrollment of an X.509v3 certificate in less than 10 seconds while spending just $120mJ$.

Reflections

My funding situation forced me to venture into cryptography-based cybersecurity, an unfamiliar knowledge domain. But what an enriching journey it was. I had to educate myself a lot of background theories while dealing with a massive amount of technical details scattered across a dozen Internet Engineering Task Force (IETF) Request for Comment (RFC) standards. After I left academia to join industry in 2018, I realized there was strong interest in moving IoT products from proprietary key management to PKI. This reassures me that the excursion I took was not just educational at the time, but will also generate value in the long term.

Because of its heavy usage of IETF standards, the work began with a clear intention to become an IETF RFC itself. And it did, after years of refinement, evolve into IETF RFC 9148 *Enrollment over Secure Transport with the Secure Constrained Application Protocol* [71].

My Contribution

The architectural design belonged to my colleague and cosupervisor Shahid. When I took over the project, there was a working prototype on the native platform implemented by Shahid's former Master students Runar and Tõmas. I was responsible for further detailed design, and the non-trivial implementation on the embedded platform. I designed and conducted the performance evaluation experiments. I contributed most of the text, tables and diagrams; Martin contributed the high-level client-server message flow (Figure 2); Shahid wrote a part of the security considerations (Section 6) and contributed dozens of comments and edits.

4. Conclusions and Future Work

This chapter wraps up the dissertation with some concluding remarks and discussions on future directions on IoT security.

4.1 Conclusions

Power-saving MAC protocols were a hot topic in the WSN research community around 15 years ago. Designers strove to minimize energy wasted on idle radio listening, by coordinating the sending and receiving of packets among neighboring nodes in time. Researchers then started to realize that, when the network is scaled up to comprise tens of nodes over a multihop routing topology, both latency and power efficiency degrade very quickly if some links become unstable due to path loss or interference, triggering excessive retransmissions at both the link layer and the higher network or transport layer. Furthermore, inefficiency caused by faulty protocol implementations can be very hard to detect using high-level performance statistics. The key network performance metrics measured under small, uncontrolled experiments are therefore hard to replicate, which hampers the adoption of low power IoT in large-scale industry applications.

Our work in are Paper I and II address directly the need for practical protocol testing tools in realistic and challenging radio environments. We have advanced the state of the art for applying controlled loss in lower power radio communication links. During our experiments with IEEE 802.15.4 radios, we discovered an important vulnerability that exposes the radio for a new type of DoS attack launched from a fellow low power transmitter. Paper III and IV demonstrate that injections of falsified PHY headers or frames are highly damaging, and we need special mitigation measures in addition to frame encryption. We have raised the awareness of PHY layer security issues in our community, and are glad to see solutions inspired by our work have already emerged [44] [45].

Another prominent trend in IoT is the uptake of standardized protocols around IPv6. Better scalability and security have gradually outweighed the performance advantages offered by proprietary architectures. We demonstrate in Paper V our efforts to enable automated, standard-based device certificate enrollment, which bring PKI one step closer to IoT. Quite a number of recent research and standardization works have pushed the frontier further along the same direction [71] [75] [80].

4.2 Future Directions

Channel hopping MAC protocols such as IEEE 802.15.4 TSCH and BLE are more robust against interference than single channel MACs such as ContikiMAC and IEEE 802.15.4 CSMA. However, given sufficient information about the channel hopping pattern, the droplet DoS attack can easily be extended to inject PHY headers on the right channel at the right time. Tiloca et al. have proposed encryption of the TSCH channel hopping sequence to defend against selective jamming [81]. It is paramount to further analyze the potential threat of channel hopping jamming or header injection against BLE's new Channel Selection Algorithm #2 (CSA#2) and develop countermeasures.

On the other hand, interest in Ultra Wide Band (UWB) radios has resurged in recent years, with a recent amendment to the IEEE 802.15.4 standard aimed at enhancing the security and accuracy with new frame formats [82]. UWB can provide range measurements in centimeter precision, enabling novel location-based IoT applications. However, UWB transceivers operate on a fixed radio channel. In particular, the globally mandatory channel 9 has so far enjoyed little interference. Chip vendors have left implementation of the MAC layer completely to the user or system developers [83]. For example, Glossy floods have been ported to UWB [84] and extended to support multiple senders in a single flood [85]. If adoption of UWB takes up pace, we can expect interference problems to emerge, due to poorly coordinated medium access and even malicious DoS attacks. Applying the knowledge we have obtained through this dissertation for development of future UWB-based IoT protocols will be very interesting.

With the strong prospect of PKI adoption by IoT, we expect new challenges and opportunities in aligning product lifecycle management with device certificate management. Avoiding operation glitches and security risks during commissioning, firmware upgrade, change of ownership, decommissioning, etc will require careful, holistic design.

Sammanfattning på Svenska

Den allmänna uppfattningen om Internet of Things (IoT) omfattar två framträdande egenskaper: 1. en mångfald av små saker, d.v.s. resursbegränsade enheter; 2. deras sömlösa integration med Internet. Banbrytande arbete inom trådlösa sensornätverk (WSN) har lagt en solid teknisk grund för autonom trådlös kommunikation med låg effekt mellan batteridrivna mikrokontrollerbaserade enheter. Dessa enheter saknar ofta ett grafiskt användargränssnitt och är därför mycket beroende av fjärrkonfiguration och mjukvaruuppgradering. Å andra sidan, eftersom en stor mängd av sådana enheter ansluts till Internet har tillsynsmyndigheter och branschexperter förknippat en enorm säkerhetsrisk med IoT. Känslig personlig information, mycket komplexa arbetsflöden och kritisk infrastruktur för allmän säkerhet står på spel.

I den här avhandlingen utforskar vi först skalbarheten av IoT. Vi studerar problemet genom att ta den särskilda vinkeln med att undersöka instabilt och felaktigt nätverksbeteende som kan uppstå när länkar mellan lågenergiradioapparater bryts. Vi ställer den specifika frågan: kan vi med hög precision emulera en otillförlitlig radiolänk med hjälp av prisvärd hårdvara? Genom att utnyttja inbyggda testlägen använder vi en lågeffektstransceiver för att generera signaler som emulerar störningar från externa källor. Detta gör det möjligt att genomföra kontrollerade experiment för att stresstesta nätverksprestandan i utmanande miljöer för radiokommunikation. Vi använder sedan radions funktionalitet för ramdetektering till att fånga upp och störa specifika ramar i luften. Resultatet av detta är en utökad testtäckning och upptäckter av subtila implementationsproblem. Våra praktiska lågkostnadsverktyg för att generera sådana störningar i radiokommunikationen fyller därmed ett gap mellan protokolldesign och testning.

Vi belyser därefter hoten från nya typer av attacker mot det fysiska lagret hos radioapparater med låg effekt, vilka kan leda till överbelastning och batteridränering i IoT-enheterna. I vårt arbete undersöker vi specifikt följande tes: radions automatiska ramavkodning kan oavsiktligt öppna dörren för tillgänglighetsattacker. Genom att injicera pakethuvuden för fysiska lager kan en skadlig programvara skapad av oss maskera sin radiosignal som autentisk trafik. Detta leder till att andra radioapparater inom radions räckvidd slösar värdefull bandbredd och energi på grund av onödig ramavkodning för de injicerade pakethuvuden. På liknande sätt kan en angripare injicera förfalskade ramar av minimal storlek till ett IoT-nätverk baserat på ett mediumåtkomstprotokoll för snabb översvämnning. Dess robusta översvämningsmekanism blir därmed kapad och tjänar i stället syftet att överväldiga hela nätverket med skräpdata. Dessa attacker, som lanseras från hårdvara med låg kostnad, är strömsnåla, svåra att upptäcka och har längre räckvidd än vanliga störningsattacker.

Slutligen tar vi ett steg närmare förverkligandet av säker och storskalig användning av IoT. IoT-data måste skyddas med kryptering, men att tilldela olika krypteringsnycklar för varje möjlig motpart på en IoT-enhet kan ha en hög kostnad vad gäller förbrukning av enhetens begränsade resurser. Med detta syfte i åtanke ställer vi följande fråga: kan vi tillhandahålla en unik och enkelt verifierbar digital identitet till varje IoT-enhet, så att den kan utbyta information på ett säkert sätt med vilken annan IoT-enhet som helst, samt med vilken värddator som helst på Internet? För att uppnå detta trots många IoT-enheters betydande resursbegränsningar anpassar vi EST-protokollet (Enrollment over Secure Transport) för en IPv6-baserad IoT-protokollstack med Constrained Application Protocol (CoAP), Datagram Transport Layer Security (DTLS) och IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN). Vår lösning, som är både minneseffektiv och energieffektiv, skyddar kommunikationen mellan IoT-enheter och certifikatauktoriteter från avlyssning och manipulering genom att tillämpa bästa praxis för kryptografi.

Vårt arbete i denna avhandling, som täcker det fysiska lagret och det applikationslagret, har berikat kunskapsdomänen för IoT-säkerhet och avancerat den tekniska gränsen för skalbar spridning av IoT-tillämpningar. Vi har även inspirerat andra att komma med nya verktyg för att generera störningar, motåtgärder mot tillgänglighetsattacker på det fysiska lagret och ytterligare optimeringar av certifikatregistrering för IoT.

Bibliography

[1] Yafei Li, Zhitao He, Thiemo Voigt, and Sanna Leidelöf. “A software radio-empowered sensor network”. In: *9th Scandinavian Workshop on Wireless Adhoc Networks (Adhoc’09)*. 2009.

[2] United Nations Department for Economic and Social Affairs. *World Population Prospects 2022: Summary of Results*. UN, 2023.

[3] Stein Emil Vollset et al. “Fertility, mortality, migration, and population scenarios for 195 countries and territories from 2017 to 2100: a forecasting analysis for the Global Burden of Disease Study”. In: *The Lancet* 396.10258 (2020), pp. 1285–1306.

[4] Jean-Philippe Vasseur. *Terms used in routing for low-power and lossy networks*. Tech. rep. IETF, 2014.

[5] IEEE Computer Society. *IEEE Standard for Low-Rate Wireless Networks*. IEEE Standard 802.15.4-2020. 2020.

[6] *Bluetooth Core Specification v5.3, Vol 6: Low Energy Controller*. Tech. rep. Bluetooth SIG, 2021.

[7] Texas Instrument. *CC2420 Datasheet (rev. 1.41b)*. 2007.

[8] *nRF52840 Product Specification v1.7*. Nordic Semiconductor. 2021.

[9] Fredrik Osterlind, Adam Dunkels, Joakim Eriksson, Niclas Finne, and Thiemo Voigt. “Cross-level sensor network simulation with cooja”. In: *Proceedings. 2006 31st IEEE conference on local computer networks*. IEEE. 2006, pp. 641–648.

[10] *ZigBee Specification Revision 22*. Tech. rep. ZigBee Alliance, 2017.

[11] *Thread Group*. `https://www.threadgroup.org`. Accessed: 2023-10-25.

[12] *nRF5340 Product Specification v1.2*. Nordic Semiconductor. 2021.

[13] *The Contiki-NG operating system*. `https://www.contiki-ng.org`. Accessed: 2023-10-25.

[14] Roman Lim, Federico Ferrari, Marco Zimmerling, Christoph Walser, Philipp Sommer, and Jan Beutel. “FlockLab: A Testbed for Distributed, Synchronized Tracing and Profiling of Wireless Embedded Systems”. In: *Proceedings of ACM/IEEE IPSN*. 2013.

[15] *Eclipse Californium CoAP FrameworkThe*. `https://projects.eclipse.org/projects/iot.californium`. Accessed: 2023-10-25.

[16] Max Pritikin, Peter Yee, and Dan Harkins. *Enrollment over Secure Transport*. RFC 7030. IETF, 2013.

[17] ITU-R. “Technical and Operating Parameters and Spectrum Use for Short-range Radiocommunication Devices”. In: *ITU-R Spectrum Management Series* (2022).

[18] CEPT. “ERC Recommendation 70-03 Relating to the Use of Short Range Devices (SRD)”. In: *ERC/REC* (2021).

[19] ETSI. “ETSI EN 300 328 Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz band; Harmonised Standard for access to radio spectrum, V2.2.2”. In: *Harmonised European Standard* (2019).

[20] FCC. “Code of Federal Regulations (CFR) Title 47 Telecommunication, Part 15 Radio Frequency Devices”. In: *Code of Federal Regulations* (2021).

[21] Radhakrishnan Natarajan, Pouria Zand, and Majid Nabi. “Analysis of coexistence between IEEE 802.15.4, BLE and IEEE 802.11 in the 2.4 GHz ISM band”. In: *IECON 2016-42nd Annual Conference of the IEEE Industrial Electronics Society*. IEEE. 2016, pp. 6025–6032.

[22] ETSI. “ETSI EN 300 440 Short Range Devices (SRD); Radio equipment to be used in the 1 GHz to 40 GHz frequency range; Harmonised Standard for access to radio spectrumWideband transmission systems, V2.2.1”. In: *Harmonised European Standard* (2018).

[23] *CC2674P10 Datasheet Rev. A*. Texas Instrument. 2023.

[24] *nRF21540 Product Specification v1.2*. Nordic Semiconductor. 2022.

[25] *System Reference document (SRdoc); Data Transmission Systems using Wide Band technologies in the 2,4 GHz band*. V1.1.1. ETSI. 2021.

[26] Matthias Schulz, Daniel Wegemer, and Matthias Hollick. *Nexmon: The C-based Firmware Patching Framework*. 2017. URL: `https://nexmon.org`.

[27] Markus Schuß, Carlo Alberto Boano, Manuel Weber, Matthias Schulz, Matthias Hollick, and Kay Römer. “JamLab-NG: Benchmarking Low-Power Wireless Protocols under Controllable and Repeatable Wi-Fi Interference.” In: *EWSN*. 2019, pp. 83–94.

[28] Matthias Schulz, Francesco Gringoli, Daniel Steinmetzer, Michael Koch, and Matthias Hollick. “Massive reactive smartphone-based jamming using arbitrary waveforms and adaptive power control”. In: *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 2017, pp. 111–121.

[29] Theodore S Rappaport. *Wireless communications: Principles and practice, 2/E*. Prentice Hall, 2002.

[30] ITU-R. “Propagation data and prediction methods for the planning of indoor radiocommunication systems and radio local area networks in the frequency range 300 MHz to 450 GHz”. In: *ITU-R Radiowave Propagation Series* (2023).

[31] David Cypher. *NIST Smart Grid Interoperability Panel Priority Action Plan 2: Guidelines for Assessing Wireless Standards for Smart Grid Applications*. Tech. rep. NIST, 2014.

[32] Jerry Zhao and Ramesh Govindan. “Understanding packet delivery performance in dense wireless sensor networks”. In: *Proceedings of the 1st international conference on Embedded networked sensor systems*. 2003, pp. 1–13.

[33] Octav Chipara, Gregory Hackmann, Chenyang Lu, William D Smart, and Gruia-Catalin Roman. “Practical modeling and prediction of radio coverage of indoor sensor networks”. In: *Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks*. 2010, pp. 339–349.

[34] Carlo Alberto Boano, Thiemo Voigt, Claro Noda, Kay Romer, and Marco Zúñiga. “Jamlab: Augmenting sensornet testbeds with realistic and controlled interference generation”. In: *Information Processing in Sensor Networks (IPSN), 2011 10th International Conference on*. IEEE. 2011, pp. 175–186.

[35] Kaishun Wu, Haoyu Tan, Hoilun Ngan, Yunhuai Liu, and Lionel M Ni. “Chip error pattern analysis in IEEE 802.15. 4”. In: *IEEE Transactions on Mobile Computing* 11.4 (2011), pp. 543–552.

[36] Krijn Leentvaar and Jan Flint. “The capture effect in FM receivers”. In: *IEEE Transactions on Communications* 24.5 (1976), pp. 531–539.

[37] Kamin Whitehouse, Alec Woo, Fred Jiang, Joseph Polastre, and David Culler. “Exploiting the capture effect for collision detection and recovery”. In: *The Second IEEE Workshop on Embedded Networked Sensors, 2005. EmNetS-II.* IEEE. 2005, pp. 45–52.

[38] Jeongkeun Lee, Wonho Kim, Sung-Ju Lee, Daehyung Jo, Jiho Ryu, Taekyoung Kwon, and Yanghee Choi. “An experimental study on the capture effect in 802.11 a networks”. In: *Proceedings of the second ACM international workshop on Wireless network testbeds, experimental evaluation and characterization*. 2007, pp. 19–26.

[39] F. Ferrari, M. Zimmerling, L. Thiele, and O. Saukh. “Efficient network flooding and time synchronization with Glossy”. In: *Information Processing in Sensor Networks (IPSN)*. 2011.

[40] Thomas Schmid. *Gnu radio 802.15. 4 en-and decoding*. Tech. rep. UCLA NESL Technical Report, 2005.

[41] Evan Faulkner, Zelin Yun, Shengli Zhou, Zhijie J Shi, Song Han, and Georgios B Giannakis. “An advanced gnu radio receiver of ieee 802.15. 4 oqpsk physical layer”. In: *IEEE Internet of Things Journal* 8.11 (2021), pp. 9206–9218.

[42] J. Hui and P. Thubert. *Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks*. RFC 6282. IETF, 2011.

[43] John Bellardo and Stefan Savage. “802.11 denial-of-service attacks: real vulnerabilities and practical solutions”. In: *12th USENIX Security Symposium (USENIX Security 03)*. 2003.

[44] Konrad-Felix Krentz, Christoph Meinel, and Maxim Schnjakin. “POTR: practical on-the-fly rejection of injected and replayed 802.15. 4 frames”. In: *2016 11th International Conference on Availability, Reliability and Security (ARES)*. IEEE. 2016, pp. 59–68.

[45] Konrad-Felix Krentz, Christoph Meinel, and Hendrik Graupner. “Countering Three Denial-of-Sleep Attacks on ContikiMAC.” In: *EWSN*. Vol. 17. 2017, pp. 108–119.

[46] Konrad-Felix Krentz and Christoph Meinel. “Denial-of-sleep defenses for IEEE 802.15. 4 coordinated sampled listening (CSL)”. In: *Computer Networks* 148 (2019), pp. 60–71.

[47] Omprakash Gnawali, Rodrigo Fonseca, Kyle Jamieson, David Moss, and Philip Levis. “Collection tree protocol”. In: *Proceedings of the 7th ACM conference on embedded networked sensor systems*. 2009, pp. 1–14.

[48] Omprakash Gnawali, Rodrigo Fonseca, Kyle Jamieson, Maria Kazandjieva, David Moss, and Philip Levis. “CTP: An efficient, robust, and reliable collection tree protocol for wireless sensor networks”. In: *ACM Transactions on Sensor Networks (TOSN)* 10.1 (2013), pp. 1–49.

[49] Tim Winter et al. *RPL: IPv6 routing protocol for low-power and lossy networks*. RFC 6550. IETF, 2012.

[50] Philip Levis, Neil Patel, David Culler, and Scott Shenker. “Trickle: A self-regulating algorithm for code propagation and maintenance in wireless sensor networks”. In: *Proc. of the 1st USENIX/ACM Symp. on Networked Systems Design and Implementation*. Vol. 25. 2004, pp. 37–52.

[51] Philip Levis, Thomas Clausen, Jonathan Hui, Omprakash Gnawali, and JeongGil Ko. *The trickle algorithm*. Tech. rep. IETF, 2011.

[52] Jiakang Lu and Kamin Whitehouse. “Exploiting the capture effect for low-latency flooding in wireless sensor networks”. In: *Proceedings of the 6th ACM conference on Embedded network sensor systems*. 2008, pp. 409–410.

[53] Jiakang Lu and Kamin Whitehouse. “Flash Flooding: Exploiting the Capture Effect for Rapid Flooding in Wireless Sensor Networks”. In: *Proceedings of IEEE INFOCOM 2009*. 2009, pp. 2491–2499. DOI: 10.1109/INFCOM.2009.5062177.

[54] Federico Ferrari, Marco Zimmerling, Lothar Thiele, and Olga Saukh. “Efficient network flooding and time synchronization with glossy”. In: *Proceedings of the 10th ACM/IEEE International Conference on Information Processing in Sensor Networks*. IEEE. 2011, pp. 73–84.

[55] Federico Ferrari, Marco Zimmerling, Luca Mottola, and Lothar Thiele. “Low-power wireless bus”. In: *Proceedings of the 10th ACM Conference on Embedded Network Sensor Systems*. 2012, pp. 1–14.

[56] Olaf Landsiedel, Federico Ferrari, and Marco Zimmerling. “Chaos: Versatile and efficient all-to-all data sharing and in-network processing at scale”. In: *Proceedings of the 11th ACM Conference on Embedded Networked Sensor Systems*. 2013, pp. 1–14.

[57] Marco Zimmerling, Luca Mottola, and Silvia Santini. “Synchronous transmissions in low-power wireless: A survey of communication protocols and network services”. In: *ACM Computing Surveys (CSUR)* 53.6 (2020), pp. 1–39.

[58] Kasun Hewage, Shahid Raza, and Thiemo Voigt. “An experimental study of attacks on the availability of glossy”. In: *Computers & Electrical Engineering* 41 (2015), pp. 115–125.

[59] Michael Baddeley, Usman Raza, Aleksandar Stanoev, George Oikonomou, Reza Nejabati, Mahesh Sooriyabandara, and Dimitra Simeonidou. “Atomic-SDN: Is synchronous flooding the solution to software-defined networking in IoT?” In: *IEEE Access* 7 (2019), pp. 96019–96034.

[60] Charles Lockie, Ioannis Mavromatis, Aleksandar Stanoev, Yichao Jin, and George Oikonomou. “Securing Synchronous Flooding Communications: An Atomic-SDN Implementation”. In: *EWSN*. 2022, pp. 250–255.

[61] Maria Rita Palattella, Nicola Accettura, Xavier Vilajosana, Thomas Watteyne, Luigi Alfredo Grieco, Gennaro Boggia, and Mischa Dohler. “Standardized protocol stack for the internet of (important) things”. In: *IEEE communications surveys & tutorials* 15.3 (2012), pp. 1389–1406.

[62] Zach Shelby, Klaus Hartke, and Carsten Bormann. *The constrained application protocol (CoAP)*. RFC 7252. IETF, 2014.

[63] Eric Rescorla and Nagendra Modadugu. *Datagram Transport Layer Security Version 1.2*. RFC 6347. http://www.ietf.org/rfc/rfc6347.txt. IETF, 2012.

[64] Göran Selander, John Mattsson, Francesca Palombini, and Ludwig Seitz. *Object security for constrained restful environments (oscore)*. Tech. rep. IETF, 2019.

[65] Open Mobile Alliance. *LwM2M core specification*. Technical Specification OMA-TS-LightweightM2M_Core-V1_2-20201110-A. Open Mobile Alliance, 2020.

[66] Open Mobile Alliance. *LwM2M transport specification*. Technical Specification OMA-TS-LightweightM2M_Transport-V1_2-20201110-A. Open Mobile Alliance, 2020.

[67] European commission. "Commission Delegated Regulation (EU) 2022/30 Supplementing Directive 2014/53/EU on Radio Equipment: Strengthening Cybersecurity, Privacy and Personal Data Protection of Wireless Devices". In: *EC Directive* (2022).

[68] ETSI. "ETSI EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements V2.1.1". In: *European Standard (EN)* (2020).

[69] Pei-Yih Ting, Jia-Lun Tsai, and Tzong-Sun Wu. "Signcryption method suitable for low-power IoT devices in a wireless sensor network". In: *IEEE Systems Journal* 12.3 (2017), pp. 2385–2394.

[70] Shahid Raza, Tómas Helgason, Panos Papadimitratos, and Thiemo Voigt. "SecureSense: End-to-end secure communication architecture for the cloud-connected Internet of Things". In: *Future Generation Computer Systems* 77 (2017), pp. 40–51.

[71] Peter van der Stok, Panos Kampanakis, Michael Richardson, and Shahid Raza. "EST-coaps: Enrollment over Secure Transport with the Secure Constrained Application Protocol". In: *Internet Requests for Comments, RFC Editor, RFC 9148* (2022).

[72] Carsten Bormann and Paul Hoffman. *Concise binary object representation (cbor)*. IETF RFC. IETF, 2020.

[73] Filip Forsby, Martin Furuhed, Panos Papadimitratos, and Shahid Raza. "Lightweight x.509 digital certificates for the internet of things". In: *Interoperability, Safety and Security in IoT: Third International Conference, InterIoT 2017, and Fourth International Conference, SaSeIot 2017, Valencia, Spain, November 6-7, 2017, Proceedings 3*. Springer. 2018, pp. 123–133.

[74] Göran Selander, John Preuß Mattsson, and Francesca Palombini. *Ephemeral Diffie-Hellman Over COSE (EDHOC)*. IETF draft. 2023.

[75] Joel Höglund and Shahid Raza. "LICE: Lightweight certificate enrollment for IoT using application layer security". In: *2021 IEEE Conference on Communications and Network Security (CNS)*. IEEE. 2021, pp. 19–28.

[76] Joel Höglund, Martin Furuhed, and Shahid Raza. “Lightweight certificate revocation for low-power IoT with end-to-end security”. In: *Journal of Information Security and Applications* 73 (2023), p. 103424.

[77] Carlos Pérez-Penichet, Frederik Hermans, Ambuj Varshney, and Thiemo Voigt. “Augmenting IoT Networks with Backscatter-Enabled Passive Sensor Tags”. In: *Proceedings of the 3rd Workshop on Hot Topics in Wireless*. HotWireless’16. New York, USA: ACM, 2016, pp. 23–27. DOI: 10.1145/2980115.2980132.

[78] Carlos Pérez-Penichet, Claro Noda, Ambuj Varshney, and Thiemo Voigt. “Battery-Free 802.15.4 Receiver”. In: *Proceedings of the 17th ACM/IEEE International Conference on Information Processing in Sensor Networks*. IPSN ’18. Porto, Portugal, 2018, pp. 164–175. DOI: 10.1109/IPSN.2018.00045.

[79] Carlo Alberto Boano, Thiemo Voigt, Claro Noda, Kay Romer, and Marco Zúñiga. “Jamlab: Augmenting sensornet testbeds with realistic and controlled interference generation”. In: *Information Processing in Sensor Networks (IPSN), 2011 10th International Conference on*. IEEE. 2011, pp. 175–186.

[80] Joel Höglund, Samuel Lindemer, Martin Furuhed, and Shahid Raza. “PKI4IoT: Towards public key infrastructure for the Internet of Things”. In: *Computers & Security* 89 (2020), p. 101658.

[81] Marco Tiloca, Domenico De Guglielmo, Gianluca Dini, Giuseppe Anastasi, and Sajal K Das. “Dish: Distributed shuffling against selective jamming attack in ieee 802.15. 4e tsch networks”. In: *ACM Transactions on Sensor Networks (TOSN)* 15.1 (2018), pp. 1–28.

[82] IEEE Computer Society. *Amendment 1: Enhanced Ultra Wideband (UWB) Physical Layers (PHYs) and Associated Ranging Techniques*. IEEE Standard 802.15.4-2020z. 2020.

[83] Dieter Coppens, Adnan Shahid, Sam Lemey, Ben Van Herbruggen, Chris Marshall, and Eli De Poorter. “An overview of UWB standards and organizations (IEEE 802.15. 4, FiRa, Apple): Interoperability aspects and future research directions”. In: *IEEE Access* 10 (2022), pp. 70219–70241.

[84] Diego Lobba, Matteo Trobinger, Davide Vecchia, Timofei Istomin, and Gian Pietro Picco. “Concurrent Transmissions for Multi-hop Communication on Ultra-wideband Radios”. In: *Proceedings of the 18th Conference on Embedded Networked Sensor Systems*. 2020, pp. 132–143.

[85] Matteo Trobinger, Davide Vecchia, Diego Lobba, Timofei Istomin, and Gian Pietro Picco. “One flood to route them all: Ultra-fast convergecast of concurrent flows over UWB”. In: *Proceedings of the 18th Conference on Embedded Networked Sensor Systems*. 2020, pp. 179–191.

Acta Universitatis Upsaliensis

Digital Comprehensive Summaries of Uppsala Dissertations from the Faculty of Science and Technology 2334

Editor: The Dean of the Faculty of Science and Technology

Distribution: publications.uu.se
urn:nbn:se:uu:diva-514996

ACTA UNIVERSITATIS
UPSALIENSIS
2023