Digital Comprehensive Summaries of Uppsala Dissertations from the Faculty of Science and Technology 2283

Towards Secure Synchronous Communication Architectures for Wireless Networks

KASUN HEWAGE

ACTA UNIVERSITATIS
UPSALIENSIS
2023

ISSN 1651-6214
ISBN 978-91-513-1844-8
urn:nbn:se:uu:diva-506085

UPPSALA
UNIVERSITET

Dissertation presented at Uppsala University to be publicly examined in Ångström 4001, Ångströmlaboratoriet, Lägerhyddsvägen 1, Uppsala, Monday, 18 September 2023 at 09:00 for the degree of Doctor of Philosophy. The examination will be conducted in English. Faculty examiner: Professor Matthias Hollick (Technical University of Darmstadt).

Abstract

Hewage, K. 2023. Towards Secure Synchronous Communication Architectures for Wireless Networks. *Digital Comprehensive Summaries of Uppsala Dissertations from the Faculty of Science and Technology* 2283. 65 pp. Uppsala: Acta Universitatis Upsaliensis. ISBN 978-91-513-1844-8.

The vision behind the Internet of Things (IoT) revolves around creating a connected ecosystem where devices, people, and systems collaborate seamlessly, unlocking new possibilities, improving efficiency, and enhancing our daily lives. IoT encloses many device classes, including low-power wireless devices that rely on batteries or energy harvesting. Due to the low-power nature and the instability of the wireless links, networks comprising these IoT devices are commonly known as Low-power and Lossy Networks (LLNs).

Several network-wide flooding-based communication primitives that employ synchronous transmissions have emerged as an alternative to traditional multi-hop routing, thereby creating a new dimension of LLN research. While these primitives have demonstrated superior performance in terms of latency and reliability, they have received little attention regarding network security. In this dissertation, we study the effectiveness of several attacks that strive to disrupt synchronous transmission-based protocols. Based on the findings from this work, we examine the security requirements and propose encryption and lightweight flood verification methods to protect synchronous transmission-based flooding protocols from these attacks.

Realising the IoT's vision demands employing well-established communication technologies like the Internet Protocol (IP) suite protocols to ensure interoperability. However, the IP suite protocols are not explicitly designed for low-power networks; hence using them in LLNs encounters numerous challenges. Some of my work included in this dissertation focuses on the performance issues of two widely used IP suite protocols: Transmission Control Protocol (TCP) and Datagram Transport Layer Security (DTLS). We propose to replace the conventional link layer protocols of the LLN stacks with a synchronous transmission-based protocol to enhance the reliability that TCP expects in lower layers, thereby improving the TCP performance. We introduce novel header compression mechanisms to reduce the size of DTLS messages without violating end-to-end security. Reducing the size of DTLS messages lowers the transmission overhead, improving its performance in LLNs.

Optical Wireless Communication (OWC) is a complementary technology to radio frequency communication. Specifically, visible light communication (VLC) has proven its capability to offer higher data transfer rates, enabling faster and more efficient communication. The last work of this dissertation draws inspiration from synchronous transmissions in LLNs and presents an OWC-based time synchronisation system for high-speed VLC access points to synchronise their transmissions. This time synchronisation system has a considerably lower synchronisation jitter than the widely-used Precision Time Protocol (PTP).

Keywords: Datagram Transport Layer Security, Synchronous Transmissions, Denial-of-service Attacks, Transmission Control Protocol, Communication Security, Time Synchronisation, Optical Wireless Communication, Networked Embedded Systems, Internet of Things

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

ISSN 1651-6214
ISBN 978-91-513-1844-8
URN urn:nbn:se:uu:diva-506085 (http://urn.kb.se/resolve?urn=urn:nbn:se:uu:diva-506085)

To all who are interested in my work

List of papers

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

I Shahid Raza, Hossein Shafagh, Kasun Hewage, René Hummen, and Thiemo Voigt. “Lithe: Lightweight Secure CoAP for the Internet of Things”. In: *IEEE Sensors Journal* 13.10 (2013), pp. 3711–3720. DOI: `10.1109/JSEN.2013.2277656`

II Kasun Hewage, Shahid Raza, and Thiemo Voigt. “An experimental study of attacks on the availability of Glossy”. In: *Computers & Electrical Engineering (Elsevier)* 41 (2015), pp. 115–125. DOI: `10.1016/j.compeleceng.2014.10.004`

III Kasun Hewage, Simon Duquennoy, Venkatraman Iyer, and Thiemo Voigt. “Enabling TCP in Mobile Cyber-Physical Systems”. In: *2015 IEEE 12th International Conference on Mobile Ad Hoc and Sensor Systems*. 2015, pp. 289–297. DOI: `10.1109/MASS.2015.38`

IV Kasun Hewage, Shahid Raza, and Thiemo Voigt. “Protecting Glossy-Based Wireless Networks from Packet Injection Attacks”. In: *2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems*. 2017, pp. 37–45. DOI: `10.1109/MASS.2017.67`

V Kasun Hewage and Thiemo Voigt. “Harmony: A Time Synchronisation System for Visible Light Communication Access Points”. In: *Proceedings of the 20th ACM Conference on Embedded Networked Sensor Systems*. SenSys ’22. 2022, pp. 435–447. DOI: `10.1145/3560905.3568549`

Reprints were made with permission from the publishers.

Additional peer-reviewed publications

In addition to the papers included in this dissertation, I have authored or co-authored the following papers and posters during my doctoral studies.

- Asanka Sayakkara, Namal Jayasuriya, Tharindu Ranathunga, Chathura Suduwella, Nithila Vithanage, Chamath Keppitiyagama, Kasun De Zoysa, Kasun Hewage, and Thiemo Voigt. “Poster: A Low-Cost Elephant Localization System”. In: *Proceedings of the 2017 International Conference on Embedded Wireless Systems and Networks*. EWSN ’17. 2017, pp. 226–227

- Namal Jayasuriya, Asanka Sayakkara, Chathura Suduwella, Chamath Keppitiyagama, Kasun De Zoysa, and Kasun Hewage. “"Wire is Not Dead": Wired-Backscatter Communication for Breakage Detection in Electric Fences”. In: *Proceedings of the 2017 International Conference on Embedded Wireless Systems and Networks*. EWSN ’17. Uppsala, Sweden, 2017, pp. 300–304

- Asanka Sayakkara, Namal Jayasuriya, Tharindu Ranathunga, Chathura Suduwella, Nithila Vithanage, Chamath Keppitiyagama, Kasun De Zoysa, Kasun Hewage, and Thiemo Voigt. “Eloc: Locating Wild Elephants Using Low-Cost Infrasonic Detectors”. In: *2017 13th International Conference on Distributed Computing in Sensor Systems (DCOSS)*. 2017, pp. 44–52. doi: 10.1109/DCOSS.2017.34. **Best paper award**

- Namal Jayasuriya, Tharindu Ranathunga, Kasun Gunawardana, Chamath Silva, Prabash Kumarasinghe, Asanka Sayakkara, Chamath Keppitiyagama, Kasun De Zoysa, Kasun Hewage, and Thiemo Voigt. “Resource-Efficient Detection of Elephant Rumbles”. In: *Proceedings of the 15th ACM Conference on Embedded Network Sensor Systems*. SenSys ’17. 2017. doi: 10.1145/3131672.3136982

- 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)*. 2016, pp. 1–9. doi: 10.1109/SAHCN.2016.7732971

- Kasun Hewage, Ambuj Varshney, Abdalah Hilmia, and Thiemo Voigt. “ModBulb: A Modular Light Bulb for Visible Light Communication”.

In: *Proceedings of the 3rd Workshop on Visible Light Communication Systems*. VLCS '16. 2016, pp. 13–18. doi: 10.1145/2981548.2981559

- Abdalah Hilmia, Kasun Hewage, Ambuj Varshney, Christian Rohner, and Thiemo Voigt. "Poster Abstract: BouKey: Location-Based Key Sharing Using Visible Light Communication". In: *2016 15th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*. 2016, pp. 1–2. doi: 10.1109/IPSN.2016.7460699

- Charitha Elvitigala, Eranda Tennakoon, Ayyoob Hamza, Yasith Lokuge, Kasun De Zoysa, Chamath Keppitiyagama, Venkat Iyer, Kasun Hewage, and Thiemo Voigt. "Towards a sensor system to tame the human elephant conflict". In: *2015 IEEE Sensors Applications Symposium (SAS)*. 2015. doi: 10.1109/SAS.2015.7133595

- Eranda Tennakoon, Charith Madusanka, Kasun De Zoysa, Chamath Keppitiyagama, Venkat Iyer, Kasun Hewage, and Thiemo Voigt. "Sensor-based breakage detection for electric fences". In: *2015 IEEE Sensors Applications Symposium (SAS)*. 2015. doi: 10.1109/SAS.2015.7133589

- Poshitha Dabare, Chathura Suduwella, Asanka Sayakkara, Damitha Sandaruwan, Chamath Keppitiyagama, Kasun De Zoysa, Kasun Hewage, and Thiemo Voigt. "Listening to the Giants: Using Elephant Infra-Sound to Solve the Human-Elephant Conflict". In: *Proceedings of the 6th ACM Workshop on Real World Wireless Sensor Networks*. RealWSN '15. 2015, pp. 23–26. doi: 10.1145/2820990.2821000

- Mohammed Ayyoob Ahamed Hamza, Chamath Keppitiyagama, Kasun de Zoysa, Venkatraman Iyer, Kasun Hewage, and Thiemo Voigt. "A Quadcopter Controller to Maintain Radio Link Quality". In: *Proceedings of the First Workshop on Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use*. DroNet '15. 2015, pp. 21–26. doi: 10.1145/2750675.2750678. **Best paper award**

- Thiemo Voigt, Kasun Hewage, and Per Alm. "Smartphone support for persons who stutter". In: *IPSN-14 Proceedings of the 13th International Symposium on Information Processing in Sensor Networks*. IEEE. 2014, pp. 293–294

Contents

Acknowledgements

During my long doctoral journey, I have been fortunate to receive tremendous support and assistance from many individuals who have made significant contributions in various ways.

I would like to begin by expressing my heartfelt gratitude to my supervisor, Prof. Thiemo Voigt, for his exceptional support, continuous guidance and for allowing me to explore new research ventures throughout my doctoral studies. This accomplishment would not have been possible without his encouragement, invaluable insights, remarkable patience and unwavering mentorship throughout my prolonged journey of doctoral studies. Secondly, I would like to thank my co-supervisor, Prof. Shahid Raza, for his invaluable guidance in the realm of Internet of Things security. Especially your guidance during the initial stage of my doctoral journey was crucial in enabling me to grow as a researcher.

My sincere thanks also go to all the co-authors, Dr. Venkatraman Iyer, and Dr. Simon Duquennoy, for helping to improve my work.

I would also like to extend my thanks to the former UNO group members, who were my colleagues, Dr. Ambuj Varshney, Dr. Carlos Pérez Penichet, Dr. Frederik Hermans, Sam Hylamia, George Daglaridis, and Andreas Soleiman for having helpful discussions and providing valuable feedback on my work.

I am also thankful to the CoRe group members for their help. A special thanks go to Prof. Christian Rohner for helping me to understand all sorts of complex administrative matters. Moreover, I really enjoyed our discussions on all kinds of technical/non-technical subjects. Thank you, Prof. Per Gunningberg and Laura Marie Feeney, for your constructive feedback and insightful discussions on my work. Furthermore, Per, it has been a pleasure to be an assistant in your courses. Besides them, I would like to thank Dr. Charalampos Orfanidis, Dr. Lorenzo Corneo and Wenqing Yan for your support and input. I also want to thank Ulrika Andersson at the IT department for making all the administrative tasks smoother.

Apart from that, I thank all the Division of Signals and Systems members for keeping me everyday company. It was a delight to take part in Friday morning Fika with you. I also thank the Division of Networked Embedded Systems members for all their support.

I would like to highlight the NES group members at SICS/RISE. I learned so much from you, particularly from technical discussions related to Contiki. Thank you very much, Zhitao He, Niclas Finne, Dr. Nicolas Tsiftes, Dr. Joel Höglund, Joakim Eriksson, Prof. Luca Mottola and Niklas Wirström, for providing me with early feedback on my work. Besides, I am immensely thankful

to Joel for helping me translate and write the Swedish summary of the dissertation. It has also been a pleasure to discuss ongoing research through our reading group.

Moreover, I am deeply grateful to my former advisors, Prof. Kasun De Zoysa and Dr. Chamath Keppitiyagama at the University of Colombo School of Computing, Sri Lanka, for kindling my interest in this field of studies ever since I was an undergraduate and then for paving the way to start doctoral studies.

I am sincerely grateful to my colleagues at Blixt Tech AB, including Trued Holmquist, Charlotta Holmquist, Jens Peter Schroer, Jan Johansson, Cheng-Huei Kuo, and Stevan Ilic, for their invaluable support and encouragement in the completion of my doctoral studies.

Next, my heartfelt gratitude goes to Cecilia Cederström for providing me with a home away from home when I moved to Sweden for doctoral studies. Thank you very much, Cecilia, and also Peder Strandh, for teaching me the Swedish culture and helping me in many ways. It made me easier to adapt to new life in Sweden and engage in doctoral studies with peace of mind.

I cannot forget to thank my Sri Lankan friends in Sweden for their support throughout this whole time. My get-together companions Pasan, Muditha, Sanjeewani, Wimal, Kumari, Lalith, Samanthi, Hasitha and Shishanthi; and other friends in Uppsala; your friendship is invaluable and has added a lot to my life. Thank you for keeping me company, being there to help whenever needed, and making my stay in Sweden enjoyable and remarkable. Moreover, Dilushi and Padmal, thank you for being there for me as friends as well as colleagues, helping me with my last paper experiments by lending me FPGA boards and supporting me in many ways. I also want to deeply appreciate the friendship and support of Daham, Mihiri, and other Sri Lankan friends in Stockholm.

Especially, I am forever grateful to my loving parents, who are proud of and overjoyed with all my achievements, for giving me moral support and encouragement in all my pursuits despite living thousands of kilometres away from me. I am also thankful to my sister, parents-in-law and the rest of my family and friends in Sri Lanka for loving me and supporting my journey. Last but not least, my heartiest gratitude goes to my wife and friend, Anudini, for constantly supporting me in every possible way. Thank you for encouraging, standing by, and believing in me when I needed it most. Without your support, my doctoral journey would have been impossible to complete.

Kasun Hewage
Uppsala, June 2023

This work has been funded by the Swedish Agency for Innovation Systems (Vinnova), the Swedish Foundation for Strategic Research (SSF) and the Swedish Internet Foundation.

List of Acronyms

6LoWPAN	IPv6 over Low-Power Wireless Personal Area Networks
AP	Access Point
CoAP	Constrained Application Protocol
DFT	Discrete Fourier Transform
DSP	Digital Signal Processor
DTLS	Datagram Transport Layer Security
FFT	Fast Fourier Transform
FPGA	Field-programmable Gate Array
IDFT	Inverse DFT
IETF	Internet Engineering Task Force
IFFT	Inverse FFT
IoT	Internet of Things
IP	Internet Protocol
IPv6	Internet Protocol Version 6
LED	Light-emitting Diode
LLN	Low-power and Lossy Network
LWB	Low-power Wireless Bus
MAC	Medium Access Control
MCU	Microcontroller Unit
MTU	Maximum Transmission Unit
OFDM	Orthogonal Frequency-division Multiplexing
OWC	Optical Wireless Communication
PCB	Printed Circuit Board
PHY	Physical Layer
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
PTP	Precision Time Protocol
RDC	Radio Duty Cycling
RF	Radio Frequency
RTO	Retransmission Timeout
RTT	Round-trip Time
SoC	System on Chip
TCP	Transmission Control Protocol
VLC	Visible Light Communication

Part I:
Dissertation Summary

1. Introduction

The Internet of Things (IoT) has become one of the trendiest technological shifts in the last two decades. The vision behind the IoT is to create a more connected and intelligent environment where devices and data seamlessly work together to improve our day-to-day life. IoT has a wide range of applications in providing real-time insights, including but not limited to smart homes, healthcare, agriculture, and energy management. Advancements in wireless communication technologies paved the way for IoT devices to be ubiquitous beyond conventional radio-based communication. For example, two leadless pacemaker implant devices wirelessly communicate with each other via blood and myocardial tissue to maintain synchrony [59]. In other technology, visible light is used to deliver high-speed internet connectivity to users [74].

Resource Constraints: IoT encloses many device classes, including low-power wireless devices that rely on batteries or energy harvesting. Therefore, ensuring energy-efficient operation of these devices is crucial for extending their lifespan. As the primary goal is energy saving, these devices consist of resource-constrained microcontroller units (MCUs) with limited processing power and memory. Wireless communication is one of the most significant contributors to the total energy expenditure of the device. Therefore, these devices utilise low-power and short-range radio transceivers. Due to the low-power nature and the instability of the wireless links, networks comprising these devices are commonly known as Low-power and Lossy Networks (LLNs).

The development of LLNs poses challenges due to the resource-constrained nature of hardware and the requirement for low-power communication. The low-power nature and the devices' limited processing power and memory restrict the use of fully-fledged operation systems and high-data-rate communication protocols. Therefore, LLNs often employ tailored embedded operating systems such as Contiki [67], RIOT [4], and Zephyr [29] and low-datarate communication standards such as IEEE 802.15.4 [44]. In this dissertation, all LLN-related experiments use the Contiki OS and hardware platforms having IEEE 802.15.4 radio transceivers. The IEEE 802.15.4 physical layer (PHY) operates within the radio frequency (RF) ranges of 868/915/2450 MHz, supporting a maximum transfer rate of 250 kbit/s and a maximum transmission unit (MTU) of 127 bytes.

Standardised Protocols: With the ever-increasing number of connected devices, the challenges in implementing LLNs at scale, such as data security, privacy, interoperability, and energy efficiency, have become more apparent. To this end, standardised communication and security protocols are the most desirable solution since these protocols are already in use and well-tested. For example, protocols in the Internet Protocol (IP) suite offer the highest level of interoperability, scalability, robustness and extensibility for communicating across heterogeneous networks. Similarly, Public Key Infrastructure (PKI) protocols enable secure authentication, encryption, and integrity. Due to its vast address space, scalability, and enhanced future-proofing, the Internet Protocol Version 6 (IPv6) has become the dominant network layer protocol in the IP suite for LLNs. To this end, the Internet Engineering Task Force (IETF) formed the IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) working group that has defined a set of protocols to enable transmitting IPv6 packets over IEEE 802.15.4 networks. The first research work of this dissertation focuses on making the Datagram Transport Layer Security (DTLS) protocol [81], one of the secure transport layer protocols in the IP suite, efficient in LLNs without compromising end-to-end security.

Multi-hop Communication: RF spectrum is a shared communication medium. Therefore, medium access control (MAC) is necessary to control participating nodes' channel access. Moreover, radio duty cycling (RDC) is essential for reducing energy consumption. Due to the limited communication range of low-power radios, LLN nodes typically rely on mesh routing protocols to communicate with nodes beyond their immediate vicinity. The routing protocol updates the forwarding table of each node, providing next-hop information to which the node forwards the received packet to reach its final destination. Another approach that achieves the same task is network-wide flooding [58]. In network-wide flooding, nodes re-broadcast the received packet until it reaches the furthest nodes of the network. Network-wide flooding with synchronous transmissions demonstrates that it can outperform mesh routing protocols in latency and reliability while having MAC and RDC built-in [28]. Most of this dissertation's research work centres on network-wide flooding with synchronous transmissions. Notably, the dissertation explores its security and privacy issues and its utilisation to enhance the Transmission Control Protocol (TCP) performance in LLNs.

Optical Wireless Communication: Optical wireless communication (OWC)[1] is a complementary technology to RF communication. Visible light communication (VLC), a type of OWC, draws attention due to its ability to provide illumination and communication by the same system. Unlike RF waves, visible light propagates in line-of-sight, preventing the medium access contention from non-line-of-sight devices. Moreover, the visible light spectrum is entirely unregulated and safe to use, especially in environments susceptible to electromagnetic interference. VLC systems leveraging modern light-emitting diode (LED) technologies demonstrate high bit rates in the order of Gbit/s [19, 94]. Deploying VLC systems with multiple access points (APs) for illumination and communication faces several challenges. For example, time synchronis-

[1] The optical wireless spectrum comprises infrared (IR), visible light and ultraviolet spectrums.

ing VLC APs is crucial to control channel access. The last research work in this dissertation extends the concept of synchronous transmissions in LLNs to OWC networks to increase the accuracy of time-synchronising VLC APs.

1.1 Research Questions

This dissertation primarily focuses on the challenges of improving performance and addressing security concerns in LLN protocols. Additionally, the dissertation explores the feasibility and potential application of LLN protocol concepts beyond LLNs.

Enhancing performance of IP suite protocols

The designs of the protocols in the IP suite do not specifically consider the constraints present in LLNs. For example, the size of the IPv6 packet header alone is 40 bytes, occupying 32 % of the IEEE 802.15.4 MTU (127 bytes). Therefore, the 6LoWPAN working group at the IEFT standardised header compression mechanisms to reduce the size of the IPv6 and some of the upper layer protocol headers [91]. While header compression certainly improves transmission efficiency due to the reduced header size, the lossy nature of low-power communication still hinders the efficiency of upper-layer protocols. For example, the community has discouraged using TCP, the widely used transport protocol in the IP suite [6], in LLNs due to the prevailing perception of its poor performance [23, 25, 47, 69, 70]. In this dissertation, we explore the research question: *Can we improve TCP performance by providing reliability in lower-layer protocols?*

The poor TCP performance has made the User Datagram Protocol (UDP) the de facto transport protocol for LLN applications. For example, the IETF standardised Constrained Application Protocol (CoAP), a UDP-based specialised web transfer protocol for LLNs [87]. The CoAP specification recommends using the DTLS [81] protocol to ensure communication security. DTLS is the UDP derivation of the TCP-based Transport Layer Security (TLS) protocol [78]. Similar to IPv6, DTLS is also not designed for LLNs. Initiating a secure session in DTLS is communication intensive and has considerable transmission overhead. Moreover, the large DTLS messages may get fragmented at lower-layer protocols leading to packet fragmentation attacks [36, 40]. Within this context, this dissertation examines the research question: *How can we enhance DTLS performance for LLNs while minimising packet fragmentation whenever feasible?*

Protecting synchronous transmissions

Glossy is an LLN flooding protocol that employs synchronous transmissions [28]. It is topology independent and provides highly reliable and low-latency communication accompanied by built-in time synchronisation with microsecond accuracy. Glossy exploits the radio receiver's ability to decode a packet without errors from several transmitters' concurrent transmissions of the same packet. Therefore, Glossy requires transmitters to synchronise their transmissions tightly to reduce reception errors at the receivers.

Glossy is not designed as a secure protocol. Therefore, Glossy is vulnerable to unauthorised eavesdropping and attacks that disrupt legitimate network operations. In this dissertation, we explore the research question: *What types of attacks can Glossy be vulnerable to, and how can we protect Glossy-based protocols from them?*

Synchronous transmissions beyond LLNs

OWC has emerged as a complementary technology to RF communication. Unlike the RF spectrum, the optical frequency spectrum is mostly unregulated and safe to use in environments sensitive to electromagnetic interference. OWC systems benefit from line-of-sight propagation of light signals to mitigate interference from other transmitters [76]. However, this characteristic limits the coverage of the OWC system. In response to this limitation, several studies have proposed multi-hop OWC systems [62]. Due to the hidden node problem, multi-hop OWC systems typically require rather complex MAC and routing strategies [48, 49].

In conventional RF synchronous transmissions, nodes wait until the reception of the entire packet before retransmission [98]. In contrast to this paradigm, Oostvogels et al. proposed a novel OWC paradigm called Zero-Wire [68]. It utilises symbol-level synchronous transmissions to send individual symbols of a packet across the network without nodes having to wait for the complete packet reception. Nevertheless, to the best of our knowledge, a conventional synchronous transmission system does not exist for OWC. Therefore, this dissertation explores the research question: *Can we use synchronous transmissions in OWC to deliver comparable performance as its RF-based counterparts?*

1.2 Methods

All the research work included in this dissertation is experimental. The main intention of the experimental approach is to quantitatively assess or characterise various aspects of the solutions to the research questions in real-world hardware environments. We use the iterative scientific method for experimental research to accomplish this objective: hypothesis formulation, experiment design, result analysis and reformulating the initial hypothesis if needed, thereby repeating previous steps.

The experiments conducted in this research work primarily involve embedded software implementations on top of commercially available LLN device platforms. In Paper I, we utilise WiSMote, equipped with an MSP430 5-Series

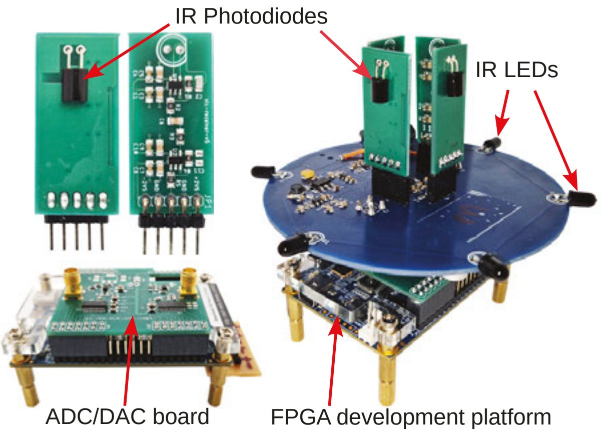

Figure 1.1. The custom OWC device platform used for the experiments in Paper V.

MCU featuring 128/16 kB of flash/RAM, to evaluate the performance of the software implementation. We adapt the original Glossy implementation for the Tmote Sky platform [20] to emulate the attacks on Glossy in Paper II. The Tmote Sky platform has an MSP430 MCU with 48/10 kB of flash/RAM. In Paper III, we modify the original Low-power Wireless Bus (LWB) [27] implementation to incorporate it with the uIP stack [23]. Paper III also uses a line-following robot to mimic a mobile LLN node. In Paper IV, we implement Glossy and LWB for the Zolertia Firefly node [99] equipped with a TI CC2538 32-bit MCU with 512/32 kB of flash/RAM to leverage the hardware support for cryptographic algorithms. As the evaluations in Paper II, Paper III, and Paper IV intend to characterise network-wide aspects, we employ multiple testbeds, each consisting of several LLN nodes, including Flocklab [56] and two additional local testbeds, in the experiments.

In contrast to LLN device platforms, there are currently no commercially available OWC/VLC device platforms suitable for the experiments conducted in Paper V. Therefore, we build a custom device platform consisting of an OWC transceiver and a digital signal processor (DSP). Figure 1.1 shows the OWC transceiver built from scratch with several printed circuit boards (PCBs) and discrete electronic components. We use a Field-programmable Gate Array (FPGA) development platform as the DSP and co-develop the required DSP steps using the Verilog hardware description language.

1.3 Contributions

The contributions of this dissertation primarily focus on addressing performance and security issues related to IEEE 802.15.4-based LLNs. Moreover, we extend the scope of our contributions beyond LLNs by applying insights and inspirations from LLN protocols to enhance the time synchronisation accuracy in OWC systems.

We address the research questions mentioned in Section 1.1 through five research papers. In addition to the contributions presented in the research papers, we make most of the software and hardware implementations publicly available[2] for reproducibility and in the spirit of fully sharing the acquired knowledge.

Header compression for DTLS messages

We propose novel header compression mechanisms to reduce the size of DTLS messages without violating end-to-end security (Paper I). We derive our header compression mechanisms from the next header compression scheme defined in the 6LoWPAN compression format [91]. Reducing the size of DTLS messages lowers the transmission overhead and avoids IP packet fragmentation at the 6LoWPAN adaptation layer.

Synchronous transmissions as a link layer for 6LoWPAN

We propose synchronous transmission protocols to replace conventional MAC and RDC protocols in the 6LoWPAN protocol stack (Paper III). To achieve this objective, we integrate LWB, which utilises Glossy floods as the underlying mechanism, with uIP [23], a widely used 6LoWPAN protocol stack. This integration aims to provide a dependable link layer for upper-layer protocols such as TCP. Moreover, the integration also eliminates the need for multi-hop routing protocols since LWB natively supports multiple traffic patterns, such as one-to-many, many-to-one, and many-to-many.

Protecting synchronous transmissions

We study the effectiveness of several attacks that strive to disrupt the synchronous transmissions used by Glossy on an LLN testbed (Paper II). The attacker nodes specifically attempt to disrupt the synchronicity of the transmissions by introducing a slight delay and modifying the content of the retransmitted packets. Additionally, we investigate other physical layer denial-of-service attacks, including jamming on Glossy.

Drawing on the findings of Paper II, we examine the security requirements of Glossy-based protocols and identify two types of adversaries (Paper IV). The first type can receive, modify, and transmit packets within the LLN, while the second type possesses the same capabilities along with access to encryption keys. We introduce encryption, lightweight flood verification and authenticated schedule dissemination methods to protect Glossy-based protocols, such as LWB, against these adversaries.

[2] `https://github.com/kasunch`

Time synchronising VLC access points

Inspired by Glossy, we present the design of a novel OWC time synchronisation system that utilises synchronous transmissions in the IR frequency spectrum (Paper V). This system provides a time synchronisation service for VLC APs to schedule their transmissions. Precise receiver-transmitter synchronisation is crucial for achieving accurate multi-hop time synchronisation. For this purpose, our OWC receiver uses the spectral leakage of the fast Fourier transform (FFT) to detect the start of the packet's transmission at the transmitter.

1.4 Dissertation Organisation

This dissertation comprises two parts: a comprehensive summary of the research work and reprints of the research papers included in this dissertation. The remainder of the first part consists of multiple chapters: Chapter 2 presents the necessary background information and foundations that underpin this research work. Chapter 3 outlines the summary of the research papers, accompanied by personal reflections and insights on each. Chapter 4 discusses the related work, and Chapter 5 concludes the dissertation with future directions for this research work.

2. Background

My work relies on various wireless communication standards and protocols, security standards, and modulation techniques. Understanding these concepts is necessary to thoroughly comprehend this dissertation's research questions and contributions. Therefore, this chapter outlines essential background information on these concepts, even though individual research papers may also discuss them.

2.1 Internet Protocol Suite for LLNs

This section describes the functions of different layers and protocols used in the IP suite (the TCP/IP reference model), specifically related to radio-based LLNs. Figure 2.1 illustrates the four layers of the IP suite and the widely-used protocols in LLNs.

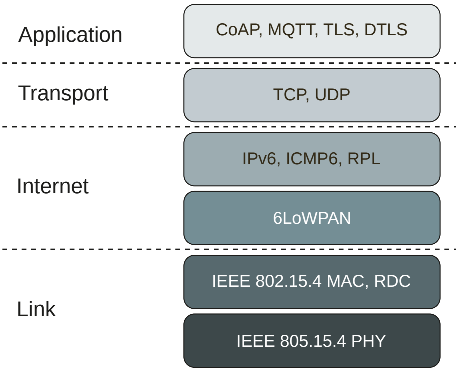

Figure 2.1. IP suite and widely-used protocols in LLNs.

The link layer consists of PHY, MAC, and RDC sub-layers. The PHY protocol defines carrier frequency, modulation techniques, and data rates. The MAC and RDC protocols manage channel access and the radio's energy consumption. The protocols in the Internet layer are primarily responsible for routing and forwarding data packets across networks. Transport layer protocols offer end-to-end data delivery, including error detection and concurrent communication multiplexing. The application layer protocols are built on top of the transport layer protocols to facilitate communication between software applications running on different devices.

In this dissertation, some of my contributions focus on improving the performance of TCP, a transport layer protocol, and DTLS, an application layer protocol in LLNs.

2.2 IEEE 802.15.4 Physical Layer

The IEEE 802.15.4 standard operates in three frequency bands: 868/915/2450 MHz supporting several modulation schemes and data rates [44]. In this dissertation, all LLN-related experiments use the 2450 MHz band and Direct-Sequence Spread Spectrum modulation scheme with Offset-Quadrature Phase-Shift Keying. As defined in the standard, each data byte is divided into 4-bit segments and mapped to one of the 16 predefined symbols such that each symbol is composed of a sequence of 32 chips. These chips are transmitted at 2 MChips/s resulting in a maximum data rate of 250 kb/s.

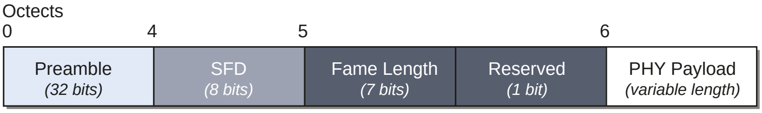

Figure 2.2. Structure of a IEEE 802.15.4 PHY frame

Figure 2.2 shows the structure of a PHY frame. The preamble is 4 bytes, and each has the value `0x00`. The start frame delimiter (SFD) is a single byte set to `0xA7`. The frame length field is 7 bits, limiting the PHY payload size (MTU) to 127 bytes. The PHY payload typically contains a 2-byte frame check sequence to detect errors, further restricting the payload size to 125 bytes.

2.3 6LoWPAN Header Compression

The IPv6 packet header is 40 bytes, occupying 32 % of the available space for the PHY payload of the IEEE 802.15.4 frame. Therefore, RFC 6282 defines a header compression mechanism to reduce the size of the IPv6 datagram [91]. Compressing headers increases the payload capacity and reduces energy consumption by reducing the number of transmitted bits.

Stateless compression is a technique employed in 6LoWPAN header compression format to compress IPv6 header fields. It involves using encoding formats to compress various fields within the IPv6 header. For instance, specific bits in the encoding format indicate whether the corresponding field in the original IP header is carried in-line or omitted in the compressed version. This approach helps to reduce the size of IPv6 headers by eliminating unnecessary or redundant information. We use this approach to compress DTLS records and handshake messages.

The RFC introduces two header encoding formats, identified by *LOWPAN_IPHC* and *LOWPAN_NHC*. The *LOWPAN_IPHC* format compresses the IPv6 header, while the *LOWPAN_NHC* format compresses subsequent headers like UDP.

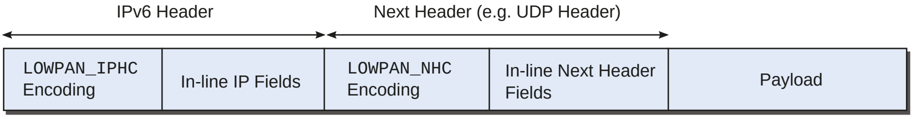

Figure 2.3. Structure of a compressed IPv6 datagram using *LOWPAN_IPHC* and *LOWPAN_NHC* encoding formats.

Figure 2.3 shows the structure of a compressed IPv6 datagram using the two header encoding formats. The *ID* bits in the *LOWPAN_NHC* encoding format (not shown in the figure) specify only the subsequent header's type and compression state. In other words, the ID bits do not specify the compression state of the UDP payload. Therefore, we chose a custom value for the ID bits to indicate both UDP and DTLS record headers use compression.

2.4 Datagram Transport Layer Security

DTLS is a UDP-based end-to-end secure communication protocol derived from the TCP-based TLS protocol [81]. While designing our header compression mechanisms, we focused on DTLS version 1.2 [80], which was the latest at the time of the work, despite the current version being 1.3 [81]. Therefore, this section outlines the essential details of DTLS version 1.2. DTLS version 1.3 introduced many backward incompatible changes, including a new handshake message exchange pattern.

Under the hood, DTLS employs a record protocol to encapsulate high-level messages into UDP payloads for communicating between endpoints. The record protocol provides confidentiality, integrity, and anti-replay protection for the data payload. It encrypts the payload using cryptographic algorithms negotiated during the handshake and handles the fragmentation and reassembly of larger messages. The handshake protocol establishes a secure connection by negotiating the security parameters. It includes a series of message exchanges between the client and server for authentication, key negotiation, and secret session key establishment.

Figure 2.4 shows different record contents and handshake messages. Only the *ClientHello* and *ServerHello* messages sent in plaintext during the initial handshake contain compressible fields. DTLS always sends the record header in plaintext. Therefore, we consider two cases for compressing the record headers: records during and after the initial handshake. Due to encryption using the negotiated cipher suite, it is not possible to inspect and compress the messages in successive re-handshakes.

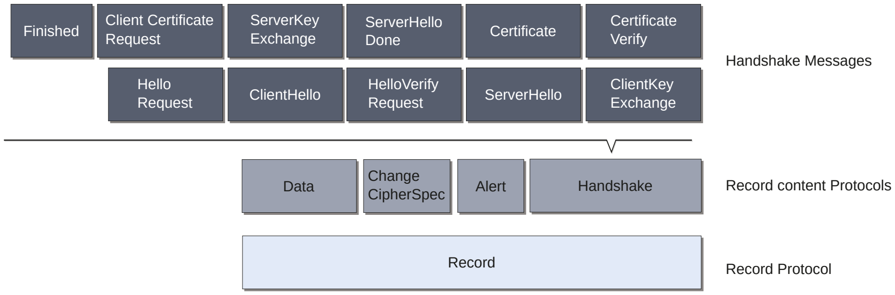

Figure 2.4. Different record contents and handshake messages used in DTLS version 1.2.

2.5 Transmission Control Protocol

TCP is the most widely used transport layer protocol in the IP suite [6]. It offers reliable, ordered, error-checked, and bidirectional data delivery between applications running on connected devices.

TCP uses the notion of a connection, where endpoints involved in the data transfer maintain certain states. These states facilitate TCP establishing, maintaining, and terminating communication between the sender and receiver. Connection establishment is the first step towards data transfer, during which the sender and the receiver synchronise their states. This process is called the three-way handshake.

TCP divides the data into smaller segments for efficient transmission. Each segment carries a sequence number to maintain the ordered data delivery. The sender waits for an acknowledgement from the recipient before sending the next segment. The absence of an acknowledgement within a specific time causes the sender to retransmit the segment. To reduce the memory footprint, most IP stack implementations for LLN devices [23, 90] have only one outstanding segment unacknowledged. The high memory capacities of modern low-power microcontrollers enable TCP implementation to increase the number of outstanding segments. However, including IP and TCP headers in every packet poses a significant overhead, making TCP inefficient in LLNs. Therefore, recent efforts toward making TCP efficient [52], including ours, rely on the frame fragmentation in the 6LoWPAN adaptation layer to reduce the header overhead.

Congestion control is one of the TCP's design features to avoid network congestion and packet losses by reducing the transmission rate. In the absence of an acknowledgement for the sent segment, the sender waits for the retransmission timeout (RTO) duration before retransmitting the same segment. The initial value of RTO is either one or three seconds [85]. RTO is estimated dynamically based on the round-trip time (RTT) between the sender and the receiver. RTT typically varies based on factors such as RDC, MAC and routing protocols, and the number of hops in the network.

Despite the common perception that TCP is ill-suited for LLNs [23, 25, 47, 69, 70], some recent efforts investigated if this perception is valid in modern LLNs [52, 55, 71].

2.6 Glossy and Low-power Wireless Bus

Conventional LLNs primarily rely on the tree-based multi-hop communication paradigm. In this communication model, nodes form a tree-like structure in their forwarding tables, specifying the next-hop information to which they forward received packets to reach the final destination. Forming and maintaining a tree-like structure involves frequent state information exchanges, such as routes to nodes. Therefore, communication protocols in this paradigm generally face challenges in scalability and mobility [45].

Ferrari et al. proposed Glossy [28] as a primitive that contrasts with the tree-based multi-hop communication paradigm. Glossy utilises network-wide flooding with synchronous transmissions for multi-hop communication. It offers highly reliable and low-latency communication with built-in support for time synchronisation within microsecond accuracy. Glossy leverages the radio receiver's ability to successfully decode a packet even when multiple transmitters concurrently transmit the same packet.

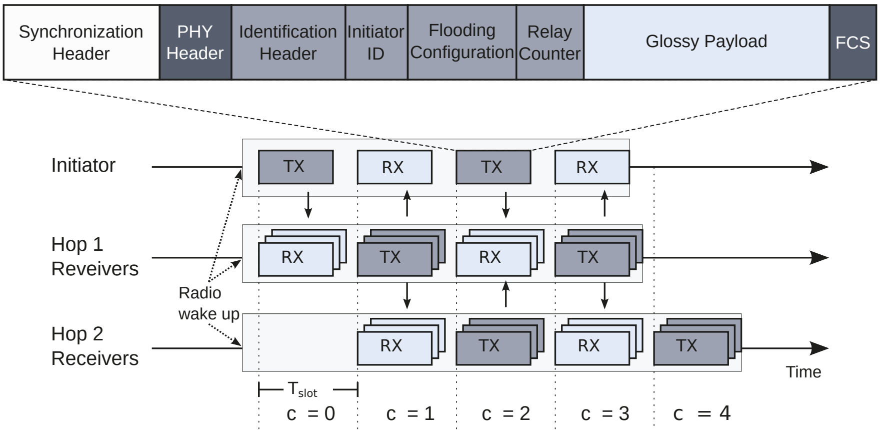

Figure 2.5. Timeline for synchronous transmissions and receptions in Glossy. Nodes increase C, the *relay counter*, before re-transmitting.

The *initiator* node starts the Glossy flood, while the other nodes act as *receivers* of the flood. Each packet in Glossy contains a field called the *relay counter*. After receiving a packet from the *initiator*, all *receivers* nodes simultaneously re-transmit the packet after increasing the value of the *relay counter*. Figure 2.5 shows the timeline for synchronous transmissions and receptions in Glossy. Nodes timestamp the reception and transmission of packets' PHY header. *T_slot* is the time duration between the start of two consecutive transmissions. It remains constant as nodes do not alter the packet length during a flood. Therefore, nodes can use the *relay counter* to compute the *reference time*, i.e., when the initiator has started the flood. Embedding the initiator's clock value in the flooded packet, and the *reference time* facilitate nodes to achieve absolute time synchronisation.

Glossy, on its own, provides only the one-to-many traffic pattern, i.e., communication from the *initiator* to the *receivers*. Therefore, Ferrari et al. introduce LWB, a scheduling protocol to control the *initiators* of the Glossy floods [27]. In LWB, a dedicated node, called the *host*, prepares a schedule of time slots for nodes in which the nodes can become the *initiators* of the Glossy flood.

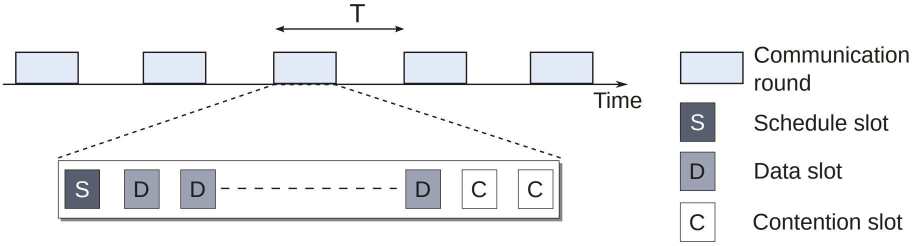

Figure 2.6. Communication rounds and time slots in LWB.

Figure 2.6 illustrates the timeline and different types of time slots used in a communication round. As depicted in the figure, the *host* disseminates the schedule to other nodes in the *schedule slot*. Then the other nodes become the *initiators* in the allocated *data slots* if they have data to send. A schedule may contain a few *contention slots* that nodes use to request to alter data slot allocation in the following schedules from the *host*. Typically, at most one such request reaches the *host* due to the capture effect [54]. As the schedule controls the Glossy floods, LWB has built-in support for RDC and MAC.

2.7 Drizzle and Arpeggio Attacks

Due to the stateless nature of Glossy, nodes in the network have to wake up their radios earlier than the anticipated time of the next flood. Therefore, the time duration between the radio wake-up and the reception of the first packet of the flood increases with the number of hops. A clever attacker can use this time duration to inject bogus packets into the network.

In the Drizzle attack, the attacker continuously injects bogus PHY frames into the LLN at a high frequency [33]. The bogus PHY frames consist of only the synchronisation header (preamble and SFD) and the frame length field with the value 127 without an actual payload. These bogus PHY frames turn the receiver into a long and futile frame decoding process, obstructing the receiver

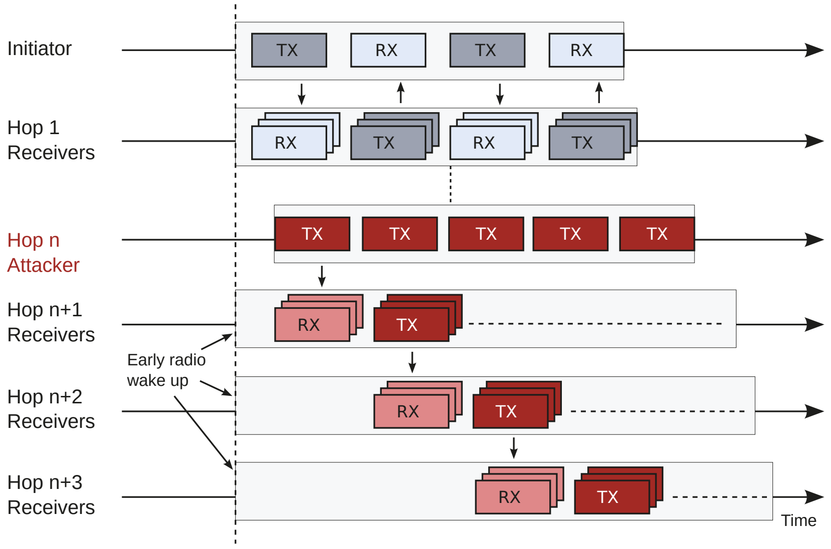

Figure 2.7. An attacker transmits bogus Glossy frames continuously without a delay between frames.

from receiving legitimate frames. However, the Drizzle attack typically affects only the attacker's neighbouring nodes.

In another work not included in this dissertation, we extend the Drizzle attack to target Glossy-based networks by embedding valid Glossy packets in the PHY frames [32]. Figure 2.7 depicts the timeline for this attack, Arpeggio, showing how an attacker can disrupt or hijack a Glossy-based network. As shown in the figure, the attacker exploits the early wake-up duration of the radios to inject bogus Glossy frames. As the nodes do not verify the received Glossy frames, the frames are propagated in the network triggering a chain reaction. Arpeggio demonstrates the attacker's ability to desynchronise an LWB network by injecting Glossy frames with bogus schedules.

2.8 Optical Wireless Communication

OWC is a complementary communication technology to conventional RF communication technologies. In OWC, nodes utilise IR, visible or ultraviolet light spectrums for communication. In the contributions, we present the design of a novel OWC time synchronisation system that utilises synchronous transmissions in the IR light spectrum.

Typically, OWC transmitters are LEDs, and the receivers are photodiodes or phototransistors. Conventional LEDs used in OWC emit incoherent light consisting of multiple wavelengths and phases. The emitted light's intensity depends on the electrical current across the LED. The coherence time, i.e., the duration during which the phase relationship between two waves remains relatively constant, is short and in the order of 10^{-13} seconds [21]. On the other hand, photodiodes or phototransistors have response times that are several orders of magnitude longer than the coherence time. Therefore, the photodiode or phototransistors detect the averaged intensities of all the light waves from the LED. Synchronously modulating the electrical current and, consequently, the light intensity of multiple LEDs with the same signal allows true constructive interference at the OWC receiver. As the transmitters modulate the intensity of the light and the receivers detect its changes, OWC is an intensity modulation with direct detection (IM/DD) system [15]. This characteristic contrasts OWC from RF communication, which modulates the phase and amplitude of the carrier signal.

2.8.1 Discrete Fourier Transform

The discrete Fourier transform (DFT) is one of the essential mathematical transformations used in designing frequency modulation methods such as orthogonal frequency-division multiplexing (OFDM). The DFT transforms a time-domain sequence of equally-spaced samples into a corresponding sequence of equal length in the frequency domain.

$$X(k) = \sum_{n=0}^{N-1} x(n) e^{\frac{-j2\pi kn}{N}}, \quad k = 0, 1, 2, \ldots, N-1 \tag{2.1}$$

Equation 2.1 defines the DFT where $x(n)$ is the n^{th} sample of the time-domain sequence as a complex number. $X(k)$ is a complex-valued function and represents the contribution of the k^{th} frequency into the time-domain sequence. N is the time-domain (or the frequency-domain) sequence length.

$$x(n) = \frac{1}{N} \sum_{k=0}^{N-1} X(k) e^{\frac{j2\pi kn}{N}}, \quad n = 0, 1, 2, \ldots, N-1 \tag{2.2}$$

The DFT is invertible. Equation 2.2 defines the inverse DFT (IDFT) that transforms a frequency-domain sequence of equally-spaced samples into a corresponding sequence of equal length in the time domain. Definitions of $x(n)$, $X(k)$ and N are the same as in Equation 2.1. OWC systems commonly use FFT and inverse FFT (IFFT) for efficient DFT and IDFT computations.

The IDFT involves complex numbers in both frequency-domain and time-domain sequences. When modulating RF signals, real and imaginary parts of the time-domain sequence independently modulate two carrier signals (in-phase and quadrature). As OWC does not employ a carrier signal, only the real part of the time-domain sequence is applicable.

$$X(k) = X(-k)^*, \quad 0 \leq k < N \text{ and } X(-k) = X(N-k) \tag{2.3}$$

One of the common techniques to obtain a real-valued sequence from IDFT, regardless of the frequency-domain sequence, is applying the conjugate symmetry (or Hermitian symmetry). Equation 2.3 defines the conjugate symmetry where $X(-k)^*$ is the complex conjugate of $X(-k)$.

We use FFT/IFFT and the conjugate symmetry in the PHY design of our OWC time synchronisation system.

2.9 Optical OFDM

OFDM is a bandwidth-efficient modulation technique that uses multiple narrowband sub-channels to transmit independent data streams in parallel. The processing steps of a typical optical OFDM system inspire the PHY design of our OWC time synchronisation system.

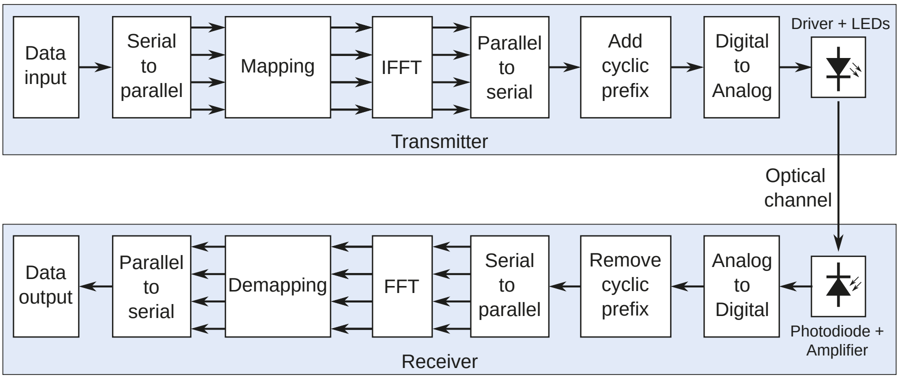

Figure 2.8. Processing steps and information flow of a typical optical OFDM system. LEDs transmit the intensity-modulated signal through the optical channel, and the photodiode receives it at the receiver.

Figure 2.8 illustrates a typical optical OFDM system's processing steps and information flow. First, the transmitter converts the input data sequence into parallel as the mapping scheme requires (e.g., quadrature amplitude modulation). After the mapping, the IFFT step transforms the frequency-domain sequence into a time-domain sequence. The two following steps serialise the time-domain sequence and add a cyclic prefix. The cyclic prefix serves as a guard interval to mitigate the inter-symbol interference. The digital-to-analogue converter produces an electrical signal based on the final data sequence. In the last step, the LED driver modulates the intensity of the LEDs by changing the electrical current flowing through them.

The receiver reverses the steps performed by the transmitter. The transimpedance amplifier converts the electrical current through the photodiode to a voltage the analogue-to-digital converter requires. After digitising the analogue signal, the next two steps involve removing the cyclic prefixed added by the transmitter and parallelising the resultant sequence. The FFT step transforms the sequence into a frequency-domain sequence. The subsequent steps include demapping the frequency-domain sequence based on the mapping scheme and serialising the resulting sequence to produce the final output data.

2.10 FFT Window Alignment

FFT implicitly assumes the input time-domain sequence to be an entire period of a continuous periodic signal in its calculations. Therefore, not meeting this requirement introduces additional frequency contents in the output of the FFT. This phenomenon is commonly known as the energy leakage (or spectral leakage) of the FFT. Properly aligning the FFT window on the time-domain signal is crucial for minimising spectral leakage and improving the performance of OFDM systems.

Bouziane et al. proposed utilising the energy leakage of the sub-channels within the misaligned FFT window to determine the correct alignment [12]. For this purpose, a few sub-channels serve as virtual sub-channels (VSCs), which do not carry any data but indicate only the energy leakage from adjacent sub-channels. If the system is free from noise, the output of the FFT, when precisely aligned, should exhibit zero energy leakage into the VSCs. In real systems affected by noise, the energy leakage into the VSCs becomes minimal when the FFT is precisely aligned. Therefore, continuously tracking the energy leakage in the VSCs enables the receiver to locate the precise alignment position in real-time.

To demonstrate the energy leakage into the VSCs, we generate a cosine signal using 64-point IFFT with $X(k = 2) = X(k = 62) = 64$ to maintain the conjugate symmetry. Then, we add a cyclic prefix to the signal by appending the first ten values of the signal to itself. We extend the signal by concatenating itself and then use the resulting signal as the input to the FFT. Figure 2.9 shows the sliding window output of the FFT for the frequency bins $X(k = 1)$, $X(k = 2)$ and $X(k = 3)$. As depicted in the figure, adding the cyclic prefix results in an abrupt transition in the time-domain signal. The figure shows energy leakage from the frequency bin $X(k = 2)$ into the adjacent bins $X(k = 1)$ and $X(k = 3)$ due to the discontinuous periodicity of the time-domain sequence when the FFT window contains the abrupt transition.

In our OWC time synchronisation system, we use the energy leakage in the VSCs to locate the correct FFT window alignment when receiving the preamble of the PHY frame.

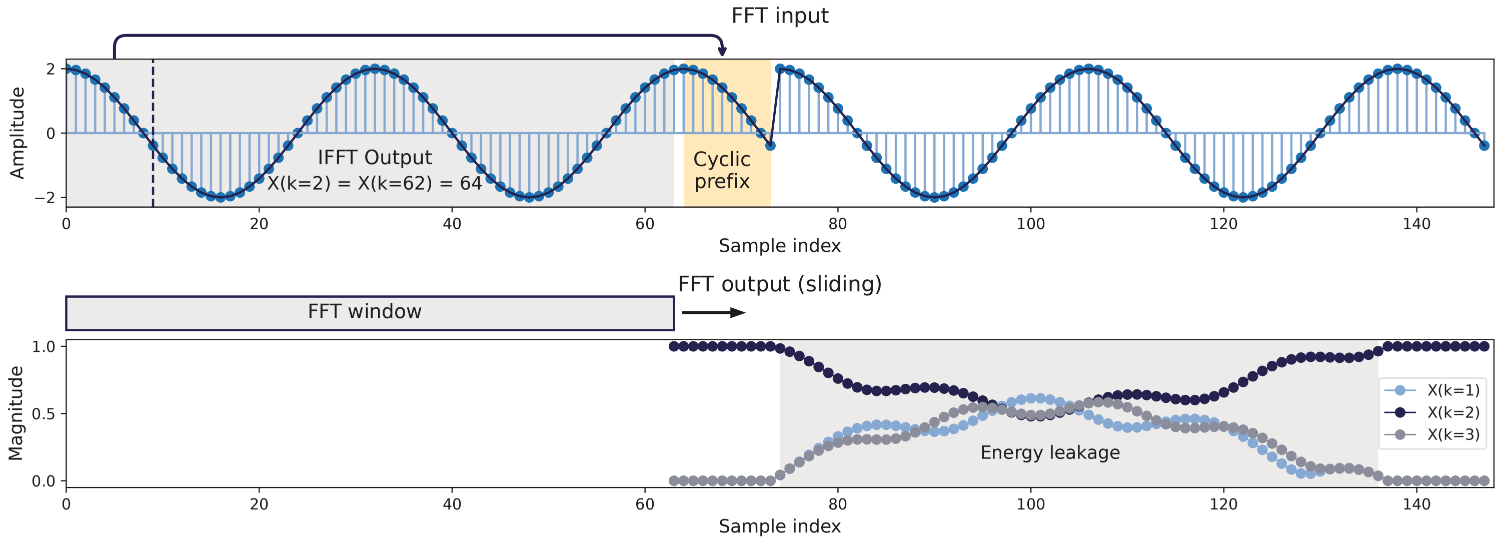

Figure 2.9. Energy leakage due to the misaligned FFT window. Adding the cyclic prefix results in an abrupt transition in the time-domain signal. Energy of the frequency bin $X(k = 2)$ leaks into the frequency bins $X(k = 1)$ and $X(k = 3)$. FFT size and length of the cyclic prefix are 64 and 10 respectively.

3. Summary of Papers

3.1 Paper I

Shahid Raza, Hossein Shafagh, Kasun Hewage, René Hummen, and Thiemo Voigt. “Lithe: Lightweight Secure CoAP for the Internet of Things”. In: *IEEE Sensors Journal* 13.10 (2013), pp. 3711–3720. DOI: 10.1109/JSEN.2013.2277656

Summary

This paper presents a DTLS integration with CoAP for IEEE 802.15.4-based LLNs. The CoAP standard specifies DTLS to secure CoAP communication. However, the design of DTLS does not specifically cater to the requirements of resource-constrained networks such as IEEE 802.15.4-based LLNs. For example, DTLS involves numerous message exchanges when initiating secure communication, increasing radio energy overhead. This paper proposes header compression mechanisms for DTLS inspired by the 6LoWPAN header compression mechanisms without compromising end-to-end security. Compressing DTLS headers reduces the size of DTLS messages and avoids packet fragmentation in lower layers. We implemented and evaluated the proposed header compression mechanisms with CoAP on Contiki OS. The evaluation shows that the DTLS header compression mechanisms significantly reduce the packet size, energy overhead, processing time and end-to-end response time.

Reflections

Despite the primary focus of this paper being on securing CoAP, the DTLS header compression mechanisms are generic and usable with any other application layer protocol that uses DTLS.

Following our work, several other studies have emerged, focusing on enhancing the performance of DTLS [35, 37, 53]. While our work focuses on compressing DTLS record headers, these studies emphasise compressing security certificates within DTLS handshake messages.

In our approach, the DTLS header compression happens at the 6LoWPAN adaptation layer. Therefore, the 6LoWPAN adaptation layer must determine whether the outgoing UDP packet’s payload is DTLS to apply the header compression. This requirement violates the most fundamental design principle of the IP stack, the layered architecture. On the other hand, compressing DTLS headers in upper layers would introduce compatibility issues in end-to-end communication.

Altogether, this work demonstrates that avoiding IP packet fragmentation considerably improves the performance of IoT protocols by reducing energy consumption and response time.

My Contribution

I implemented the 6LoWPAN-based DTLS header compression on Contiki OS and contributed to the evaluation by conducting some experiments. Moreover, I also wrote parts of the paper.

3.2 Paper II

Kasun Hewage, Shahid Raza, and Thiemo Voigt. "An experimental study of attacks on the availability of Glossy". In: *Computers & Electrical Engineering (Elsevier)* 41 (2015), pp. 115–125. DOI: `10.1016/j.compeleceng.2014.10.004`

Summary

Glossy is an LLN flooding protocol that uses synchronous transmissions without relying on topology-dependent states such as tree-like structures. It offers highly reliable and low-latency communication with built-in time synchronisation. Glossy's design does not consider the security issues of the protocol. Therefore, Glossy is vulnerable to attacks aimed at disrupting legitimate network operations. In this paper, we propose several attacks aimed at disrupting the synchronous transmissions that Glossy relies on. For this purpose, we consider three types of attacker nodes: those that retransmit packets earlier than expected, those that introduce delays in packet retransmission, and those that modify the content of Glossy packets before retransmission. We conducted experiments on a 30-node testbed, and the results reveal that Glossy is robust against attacks that do not adhere to strict timing constraints to disrupt synchronous transmissions. Nevertheless, the results also show that Glossy is most vulnerable to Glossy's relay counter modification attack rendering the nodes to lose synchronisation. The paper also discusses some countermeasures to mitigate and detect such attacks.

Reflections

Glossy-based networks are susceptible to unauthorised eavesdropping, packet modification, and attacks aimed at disrupting network operations due to the absence of built-in security mechanisms. Therefore, it is essential to study possible attacks on Glossy-based networks to design effective security services. To the best of our knowledge, this work represents the first dedicated study to investigate the security vulnerabilities of Glossy.

The main insight of this work is how Glossy achieves its superior communication reliability despite the presence of nodes that do not adhere to strict timing constraints. The capture effect, combined with multiple retransmissions, allows nodes to receive Glossy packets at least once without errors, making the overall packet reception successful.

My Contribution

Thiemo came up with the initial idea of exploring Glossy's security vulnerabilities. I implemented the attacks using the original Glossy implementation and conducted the experiments on the testbed. I am the paper's main author and wrote most parts in collaboration with the co-authors.

3.3 Paper III

Kasun Hewage, Simon Duquennoy, Venkatraman Iyer, and Thiemo Voigt. "Enabling TCP in Mobile Cyber-Physical Systems". In: *2015 IEEE 12th International Conference on Mobile Ad Hoc and Sensor Systems*. 2015, pp. 289–297. DOI: 10.1109/MASS.2015.38

Summary

This paper proposes LWB as a link layer protocol for IP stacks in 6LoWPAN-based LLNs. This work's primary objective is to enhance TCP performance by improving the reliability of the underlying layers. TCP received little attention for using it in LLNs mainly due to the common perception that TCP is not lightweight and its tendency to incorrectly infer network congestion from a single packet drop. Node mobility worsens TCP's performance problems due to the drastic changes in wireless channel dynamics. Moreover, mobility may change nodes' neighbourhoods, leading to invalid entries in nodes' forwarding tables. Using LWB as a link layer eliminates the need for routing, MAC and RDC protocols in the IP stack. This paper proposes two TCP-aware scheduling algorithms for the LWB host. We implemented LWB for Contiki OS and integrated it with uIP, a widely used 6LoWPAN IP stack. In the evaluation, we use a local testbed consisting of 14 static nodes and a node mounted on a line-following robot. The evaluation demonstrates that TCP consistently performs well in static and mobile scenarios thanks to the stateless operation of Glossy, the underlying communication primitive of LWB.

Reflections

One of the highlights of this work is the benefit of IP packet fragmentation for sending larger payloads in transport layer protocols when lower layer protocols provide reliable communication in LLNs. Note that, in Paper I, we avoid IP packet fragmentation by compressing headers due to the unreliable nature of the communication in lower layers.

In a more recent investigation, Kumar et al. attributed TCP performance issues to TCP's header overhead in sending smaller link-layer frames, the hidden terminal effect over multiple hops, and TCP's poor interaction with RDC protocols [52]. Their work achieved six times higher TCP goodput than ours in a single-hop scenario but only 1.6 times higher in a multi-hop scenario. Note that their work only considers static node placements, while ours also accounts for node mobility. In general, their approach is functionally similar to ours as they also employ IP packet fragmentation and adaptive adjustments to RDC. In our work, the LWB host changes the schedule based on the queue length of the nodes, thus changing the nodes' RDC.

In LWB, data and contention slots immediately follow the schedule slot. Therefore, the duration between the data and contention slots in consecutive schedules may be longer in highly duty-cycled networks. As a result, TCP handshakes may experience longer completion times or premature timeouts due to packet buffering. To solve this issue, the LWB host could disseminate schedules consisting of only a few contention slots more frequently; thus, nodes can promptly notify the host about the demand for data slots.

My Contribution

Thiemo conceived the initial idea to use LWB to improve the performance of TCP. Following this idea, I designed and implemented the LWB integration with the uIP stack, including the scheduling algorithms on Contiki OS. I also conducted all the experiments. I am the primary author of this paper and wrote most parts in collaboration with the co-authors.

3.4 Paper IV

Kasun Hewage, Shahid Raza, and Thiemo Voigt. "Protecting Glossy-Based Wireless Networks from Packet Injection Attacks". In: *2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems*. 2017, pp. 37–45. DOI: 10.1109/MASS.2017.67

Summary

Glossy is not designed as a secure protocol. In Paper II and another work [32], we experimentally demonstrated that Glossy-based networks are vulnerable to packet injection attacks which mimic legitimate Glossy floods. Therefore, this paper investigates the possibility of protecting Glossy-based networks from such attacks and minimising their impact on the network. To achieve this goal, we characterise challenges in securing Glossy and define security services based on the well-known CIA triad model: confidentiality, integrity, and availability. Our approach considers two types of adversaries: one with the capability only to intercept Glossy floods through sniffing and another with an extended ability to access the encryption key. Authenticated encryption of Glossy packets protects against the first type of adversaries, ensuring security services in the CIA triad. However, the second type of adversaries could still execute packet injection attacks by imitating legitimate Glossy packets, thereby compromising the network's availability. We mitigate this vulnerability using a lightweight flood verification mechanism that employs a one-way hash function. The paper describes how LWB can utilise PKI to securely initiate the flood verification mechanism. We implemented Glossy and the flood verification mechanism for a modern system-on-chip (SoC) with hardware support for authenticated encryption, one-way hash function and public-key cryptography (PKC) algorithms. The evaluation of the flood verification mechanism on a 25-node testbed demonstrated its ability to confine the impact of the packet injection attack to the attacker's single-hop nodes.

Reflections

Our biggest challenge in designing security services for Glossy was adhering to Glossy's strict timing constraints while performing cryptographic operations such as packet encryption. We addressed this challenge by leveraging hardware support in modern SoCs for cryptographic operations and precise timing.

Although Glossy is a highly efficient communication paradigm for LLNs, its security concerns received little or no attention. Apart from our work (this paper, Paper II and Arpeggio [32]), only Lockie et al. have studied security issues of Glossy-like protocols so far [57]. However, their work only focuses on encrypting packets of frequency-hopping Glossy-like protocols.

My Contribution

I analysed the requirements of security services for Glossy based on the findings in Paper II and designed the flood verification mechanism. I implemented Glossy and the flood verification mechanism on a modern SoC and conducted all the experiments. I am the main author of this paper and wrote most parts in collaboration with the two co-authors.

3.5 Paper V

Kasun Hewage and Thiemo Voigt. “Harmony: A Time Synchronisation System for Visible Light Communication Access Points”. In: *Proceedings of the 20th ACM Conference on Embedded Networked Sensor Systems*. SenSys ’22. 2022, pp. 435–447. DOI: 10.1145/3560905.3568549

Summary

This paper presents an OWC-based time synchronisation system for VLC APs. In high-speed VLC systems, APs seamlessly provide communication and illumination from the light source. Therefore, APs must synchronise their transmissions to avoid interference in light-overlapping areas. We draw inspiration from Glossy to achieve this goal and use synchronous transmissions in the IR frequency spectrum to synchronise nodes over multiple hops. In our system, the OWC transmitter modulates the intensity of the IR light using a frequency modulation technique. The OWC receiver uses FFT to decode the transmitted data in the received frequency-modulated signal. We utilise the spectrum leakage of FFT to achieve precise synchronisation between the receiver and transmitter. This synchronisation enables us to timestamp the received packets accurately. As off-the-shelf OWC transceivers are unavailable for our requirements, we design and build a custom OWC transceiver and implement DSP steps on an FPGA development platform. We also implement the synchronous transmission protocol on the FPGA platform.

In this paper, we evaluate various aspects of the OWC transceiver and the accuracy of time synchronisation over multiple hops. The evaluation demonstrates that our system can synchronise nodes up to nine hops with an average synchronisation accuracy of slightly over one hundred nanoseconds. The evaluation also shows that the synchronisation jitter is considerably lower than the Precision Time Protocol (PTP) despite its synchronisation accuracy being in the range of a few tens of nanoseconds in the best-case scenario.

Reflections

This work’s main highlight is demonstrating how synchronous transmissions can enhance the quality of timing services necessary for applications, even when the underlying communication technology differs from the initial approach. Throughout this work, we obtained a crucial insight into the importance of precise receiver-transmitter synchronisation when receiving a packet for time synchronising nodes. In summary, the modulation and demodulation techniques used in the transceiver directly impact the application-level time synchronisation accuracy.

My Contribution

I am the main author of this paper and conceived the idea behind this work. I designed the entire system and implemented the FPGA-baed DSP steps, including the synchronous transmission protocol. I also built the OWC transceiver hardware. I wrote most parts of the manuscript in collaboration with Thiemo.

4. Related Work

This chapter reviews prior and follow-up related work that contextualises this dissertation's research questions and contributions.

4.1 Compression Mechanisms for Security Protocols

In this dissertation, we present novel header compression mechanisms for DTLS records and handshake messages to reduce the transmission overhead in LLNs. Our compression approach is header specific, i.e., we compress individual fields in DTLS headers. An alternative approach to this compression method is the generic header compression (6LoWPAN-GHC) outlined in RFC 7400 [11]. However, 6LoWPAN-GHC is not specially targeted for DTLS, thus less efficient than ours. In recent work, Fragkiadakis proposed a rule-based compression mechanism for DTLS records and handshake messages [30] derived from the Static Context Header Compression for CoAP [64]. While this approach performs similarly to ours, it requires a custom DTLS implementation. The IETF has initiated drafting the Compact TLS 1.3 (cTLS) standard with similar goals to these approaches targeting both TLS and DTLS [79]. The cTLS's design includes various strategies, including omitting unnecessary values, fields, and handshake messages, compact encoding, and utilising alternative cryptographic techniques. However, cTLS uses a different over-the-wire format making it incompatible with previous TLS/DTLS versions. Banerjee et al. proposed energy-efficient DTLS (eeDTLS) that compresses DTLS packet headers in Bluetooth Low Energy networks [5]. Unlike our approach, eeDTLS uses a fixed-size encoding format for header compression and an address translation at the gateway to eliminate IPv6 and UDP headers in the packet. While our work uses header compression mechanisms, some follow-up works focus on compressing the security certificates within DTLS handshake messages [35, 37, 53].

Besides compressing DTLS records and messages, several other studies have investigated the application of header compression to various security protocols in LLNs. In earlier work, Raza et al. proposed using 6LoWPAN header compression to reduce the size of IPSec authentication and encapsulation headers [77]. The community has studied several approaches [39], including 6LoWPAN header compression [7, 84], to reduce the size of the Host Identity Protocol [65] packets. While this section only reviews the related work in the context of our work, header compression, in general, has been extensively studied over the years [92].

4.2 Performance of Transmission Control Protocol

In this dissertation, we propose to replace the conventional link layer protocols of the LLN stack with LWB to enhance the reliability that TCP relies on its lower layers. Therefore, this section reviews related work to enhance TCP performance in LLNs.

The closest work similar to ours in this context is LaneFlood which utilises Glossy floods to provide a reliable routing substrate for IP suite protocols [13]. Nevertheless, LaneFlood's evaluation does not include TCP performance measurements. LaneFlood differs from our approach by not using a scheduled control for Glossy floods and creating a path between the source and destination before the data transfer to limit the number of participating nodes. However, these features can reduce reliability in the presence of node mobility and multiple parallel data streams.

In contrast to our approach, other works to improve TCP performance in LLNs are built on link-based mesh routing protocols. Kim et al. experimentally studied TCP performance over RPL-based LLNs [50]. Their work shows that TCP suffers from unfairness and starvation depending on how RPL constructs the tree topology. For example, a heavily loaded common ancestor node could drop TCP packets due to the lack of space in the packet buffers. They also highlighted that stripped-down TCP implementations may require adaptive methods to adjust the RTO. Following this suggestion, Lim proposed a new technique for managing the TCP's retransmission timer [55] based on weak RTT estimation of CoCoA, an advanced congestion control mechanism for CoAP [8]. Along the same lines, Park et al. utilised the border router to artificially manipulate the TCP streams' RTT [72]. While this approach needs no modifications at the end nodes, it applies only to the TCP flows passing across the border router. In addition to fiddling with the RTT, others proposed caching TCP segments on intermediate nodes along the destination's path and performing local retransmissions if needed [14, 24, 41]. Duquennoy et al. demonstrated a burst forwarding mechanism for low-power radios using TCP to achieve high throughput [26]. Their work uses two Linux hosts with full-scale IP stacks at the end nodes and only uses LLN nodes for multi-hop communication. However, this work only evaluates the performance of the new burst forwarding protocol rather than TCP performance in LLNs.

In recent work, Kumar et al. demonstrated that TCP performance issues stem from TCP's incompatibilities with its lower layers, such as the link layer [52]. They proposed a series of adjustments to the network stack, including MAC and RDC protocols, to improve TCP performance. Their work achieved six times higher TCP goodput than ours in a single-hop scenario but only 1.6 times higher in a multi-hop scenario for static node placements.

To summarise, our work presented in this dissertation is the pioneering effort to tackle the underlying issue behind TCP's subpar performance in LLNs, i.e., the poor reliability provided by lower layers.

4.3 Denial-of-Service Attacks

In this dissertation, we examine the effectiveness of several attacks on synchronous transmission-based protocols and propose security measures. Despite the remarkable performance of synchronous transmissions in various other aspects, security is the least explored facet [17]. Besides our work and Arpeggio [32], only Lockie et al. investigated security issues of synchronous transmissions [57]. Their work focuses on securing synchronous transmissions in Bluetooth Low Energy networks rather than IEEE 802.15.4-based LLNs. Although their work includes payload encryption and a mechanism for nodes to join the channel-hopping network securely, it does not provide a flood verification method like ours. The rest of this section reviews related work on denial-of-service attacks (DoS) in LLNs and potential countermeasures, as the attacks presented in this dissertation specifically target the disruption of synchronous transmissions.

One of the common DoS attacks in LLNs is jamming. The community extensively explored a wide range of strategies aimed at disrupting wireless communications [2]. Among these, reactive jamming is the hardest to detect and the most energy-efficient strategy making it a severe threat to LLNs [88]. While several solutions exist to detect and complicate carrying out such attacks [3, 73, 88, 89], the attack's impact is typically confined to the neighbouring nodes since the attacks primarily aim at corrupting the received packets. Cao et al. investigated an energy depletion attack that targets encrypted LLNs [16]. They exploit the fact that nodes must receive the entire encrypted packet to verify its integrity. Without knowing the encryption key, an attacker could transmit bogus and large packets to make the receiver nodes spend their energy in a futile receiving process.

As highlighted in our work, losing time synchronisation with the *initiator* of the synchronous transmissions is the primary reason for nodes to lose packets. Although unrelated to synchronous transmissions, several studies [38, 75, 83] investigated securing the flooding time synchronisation protocol [60]. These studies propose several methods to locally identify and discard malicious values of the fields used to estimate the sender's time from received packets. In synchronous transmission protocols such as Glossy, it is possible to utilise similar techniques to detect drastic changes to the *relay counter* field in static LLNs.

Riecker et al. analysed the effect of DoS attacks on several metrics, such as received signal strength indicator, transmit/listen time and checksum errors in received packets [82]. Almon et al. extended this work to develop a lightweight intrusion detection system by analysing variations in a combination of metrics [1]. While these efforts target conventional mesh routing-based LLNs, it would be worth investigating the applicability of other metrics, including the relay counter, for detecting DoS attacks on synchronous transmission-based networks.

4.4 Multi-hop Optical Wireless Communication

In the last work of this dissertation, we use the concept of synchronous transmissions in the IR spectrum to design a multi-hop time synchronisation system for VLC APs. In this context, Zero-Wire is the closest related work to ours that uses multi-hop OWC [68]. It employs symbol-level synchronous transmissions, allowing individual symbols of a packet to be sent across the network without requiring nodes to wait for the complete packet reception. Unlike Zero-Wire, our work employs the store-and-forward packet retransmission method used in conventional RF-based synchronous transmission protocols.

Due to the directionality of the OWC transmissions, several works have studied multi-hop communication to increase coverage. Cooperative relaying of light signals is an extensively studied method to increase coverage [18, 66, 95, 97]. However, its capability is limited to single-relay, linear or triangular topologies. Klaver et al. introduced Shine, an innovative OWC system designed for distributed multi-hop communication [51]. Each node in Shine has several LEDs and four photodiodes to cover 360 degrees of field of view, enabling nodes to transmit and receive signals in multiple directions. Our hardware prototype draws inspiration from Shine's design by incorporating multiple LEDs and four photodiodes. Similarly, Schmid et al. proposed a multi-hop OWC system with Linux-enabled commercial light bulbs for IP-based communication [86]. Their work relies on the IP stack's routing protocol and uses a simplified IEEE 802.11-style MAC protocol. As others have investigated [48, 49], rather complex MAC and routing strategies are required to address the hidden node problem in multi-hop OWC.

In summary, synchronous transmissions' centralised MAC can effectively eliminate the hidden terminal problem in OWC. Moreover, the stateless network-wide flooding with synchronous transmissions also eliminates the necessity for a routing protocol, simplifying the network architecture.

4.5 Time Synchronisation

Considering that the final work of this dissertation is a multi-hop OWC time synchronisation system, this section reviews the relevant literature concerning time synchronisation protocols and systems in general.

The Network Time Protocol (NTP) [61] and PTP [43] are the IP suite's de facto time synchronisation protocols. NTP is a client-server protocol such that the client regularly requests time information from one or more servers. After receiving a response from the server, the client calculates the time offset and round-trip delay to adjust its local clock accordingly. As NTP does not consider variations in queuing time in switches and routers, it typically achieves an accuracy of only a few milliseconds. In contrast, PTP leverages the packet timestamping capability of network interface controllers to address variations in queuing time in switches and routers. Consequently, PTP requires all intermediary switches and routers in the network to be PTP compatible, resulting in a costly and intricate network setup [96]. Our work demonstrates that OWC-based synchronous transmissions can achieve higher time synchronisation performance than PTP regarding the synchronisation jitter.

Guo et al. proposed PSync, an energy-efficient VLC-based time synchronisation protocol for IoT [31]. As PSync's intention is energy efficiency, it employs a de Bruijn sequence [34] to provide a rough estimation of time using the least amount of information. Although PSync consumes less energy than sending a byte in IEEE 802.15.4-based radios, it provides time synchronisation only for star network topologies.

5. Conclusions and Future Work

This chapter presents concluding remarks regarding the work encompassed in this dissertation and outlines future directions.

5.1 Conclusions

Realising the IoT's vision demands employing well-established communication technologies like the IP suite protocols to ensure interoperability. However, IP suite protocols are not designed explicitly for energy-sensitive IoT networks like LLNs. Consequently, the community and the industry have proposed numerous adaptation techniques for IP suite protocols over the years to render them suitable for LLNs' usage. Mesh routing has been the standardised method used in IP-based LLNs to facilitate multi-hop communication. Although synchronous transmission protocols have demonstrated superior performance in latency and reliability for multi-hop communication, they have yet to receive wider attention towards integrating them with IP stacks and addressing security concerns in LLNs.

At a high level, this dissertation explores specific research questions on IoT protocol performance enhancements and security issues. It comprises five research papers that thoroughly examine these research questions and propose relevant solutions. We propose to replace the conventional link layer protocols of the LLN stacks with LWB to enhance the reliability that TCP relies on its lower layers, thereby improving the TCP performance. We introduce novel header compression mechanisms derived from the 6LoWPAN header compression format to reduce the size of DTLS messages without violating end-to-end security. Reducing the size of DTLS messages lowers the transmission overhead, improving its performance in LLNs. We examine the effectiveness of several attacks on synchronous transmission-based protocols and propose security measures, including encryption and lightweight flood verification methods, to protect from these attacks.

The final work of this dissertation concentrates on applying the concept of synchronous transmissions to OWC, while rest of the work tackles research questions within LLNs. This work presents an OWC-based time synchronisation system for high-speed VLC APs to synchronise their transmissions.

In conclusion, my work explores one approach to address selected research questions on performance improvements and security concerns in IoT protocols. Follow-up studies by others on these research questions demonstrated several alternative approaches, indicating room for further investigations. Nevertheless, I believe the insights presented in this dissertation will assist future research in LLNs and unlock new avenues in OWC.

5.2 Future Directions

Since its renowned reintroduction through Glossy [28], the community has extensively studied synchronous transmission protocols over the last decade [63, 98]. In line with these studies, most of this dissertation's research work also centres around synchronous transmission protocols. Thus, this section presents my reflections on future directions of synchronous transmission protocols.

Standardisation of Synchronous Transmissions

Synchronous transmission protocols have shown remarkable performance in terms of reliability, latencies [22], energy consumption [46], and robustness against interference from co-located networks [9]. Despite these features being key enablers for widespread adoption as an IoT network primitive, almost all of the work related to synchronous transmissions has remained within academia. In my opinion, the absence of standardisation is the primary reason for the industry's limited adoption of synchronous transmission protocols. On the contrary, the industry also holds the potential to take the lead in initiating standardisation efforts for synchronous transmission protocols. As Chang et al. pointed out [17], one approach to this end is integrating synchronous transmissions as an additional service in the IEEE 802.15.4 standard. This integration enables wireless SoC vendors to support synchronous transmissions directly in hardware, eliminating the need for intricate software implementations.

New Avenues for Synchronous Transmissions

As 5th-generation (5G) networks are being deployed worldwide, the community has already started exploring 6th-generation (6G) networks to enhance 5G's capabilities, like ultra-high data rates and ultra-low latencies [93]. In 6G, the optical spectrum has emerged as a viable alternative to the RF spectrum due to the insufficient RF bandwidth for future high data-rate communication services. Towards this purpose, Task Group 13 of the IEEE 802.15 working group has initiated the drafting process for IEEE 802.15.13, a standard focused on optical wireless personal area networks [42]. This standard aims to support data rates of multiple Gbit/s. The draft of IEEE 802.15.13 proposes using centrally coordinated medium access for all data transmissions [10]. This dissertation's last work demonstrates that synchronous transmissions in the IR spectrum can deliver the necessary time synchronisation service for VLC APs to fulfil the same purpose, i.e. coordinated MAC. I believe this work paves the way for future research on synchronous transmissions in OWC, particularly with IEEE 802.15.13 networks.

6. Sammanfattning på svenska

Sakernas Internet, även kallat IoT, har blivit ett av de mest trendriktiga teknikskiftena under de senaste två decennierna. Visionen bakom IoT är att skapa en mer sammankopplad och smart miljö, där enheter och data sömlöst arbetar tillsammans för att förbättra vårt dagliga liv. Framsteg inom trådlös kommunikation banade väg för IoT-enheter att bli tillgängliga även bortanför konventionell radiobaserad kommunikation. Till exempel så har snabba internetuppkopplingar via synligt ljus varit ett aktivt forskningsområde.

Sakernas internet har en rad tillämpningar, vilka inkluderar att trådlöst koppla upp lågenergi-enheter som är beroende av batterier eller energiinsamling. Det innebär att säkerställa energieffektivitet för dessa enheter blir avgörande för att förlänga deras livslängd. Utifrån energibesparingar som främsta mål utrustas enheterna med mikrokontroller med begränsad beräkningskapacitet och minne, samt lågenergi-radio med kort räckvidd. På grund av energibegränsningarna, och instabiliteten hos radiouppkopplingarna brukar de resulterande radionätverken kallas “Low-power and Lossy Networks”, LLN.

Med det ständigt ökande antalet uppkopplade enheter blir utmaningarna, till exempel gällande säkerhet, integritet, interoperabilitet och energieffektivitet, med att implementera LLNs i stor skala allt mer uppenbara. För att möta utmaningarna är standardiserade protokoll för kommunikation och säkerhet den mest önskvärda lösningen, eftersom protokollen redan används och är vältestade. Till exempel protokollen i internetprotokollsviten, IP, tillhandahåller den bästa tillgängliga interoperabiliteten, skalbarheten, robustheten och utbyggbarheten för kommunikation över heterogena nätverk. Tack vare sin enorma adressrymd, skalbarhet och framtida utbyggbarhet har Internet Protocol Version 6, IPv6, blivit det vanligaste valet för nätverkslagret i LLN. Internet Engineering Task Force, IETF, har skapat en arbetsgrupp, IPv6 over Low-Power Wireless Personal Area Networks, 6LoWPAN, som har tagit fram protokoll för IPv6-trafik över IEEE 802.15.4-nätverk.

På grund av den begränsade räckvidden hos lågenergi-radio så är LLN-enheter vanligtvis beroende av nätverksfunktioner som meshrouting för att nå andra enheter utanför den omedelbara närheten. En annan nätverksfunktion som kan utföra samma uppgift är flooding. I en total flooding av ett nätverk så upprepar enheterna utskickandet av mottagna radiopaket tills även de mest avlägsna enheterna har fått trafiken. Glossy är ett protokoll för flooding som använder synkroniserade överföringar, och har i utvärderingar visats kunna överträffa meshrouting i fråga om latens och pålitlighet.

Designen av protokoll i IP-sviten tar inte särskild hänsyn till de begränsningar som finns i LLN. Transmission Control Protocol, TCP, rekommenderas inte för LLN på grund av en rådande uppfattning om dess dåliga prestanda över opålitliga radioförbindelser. I denna avhandling föreslår vi att ersätta de konventionella länklager-protokollen i 6LoWPAN-stacken med Low-power Wireless Bus, LWB, ett Glossybaserat protokoll. LWB tillhandahåller den pålitlighet som TCP förväntar sig av länklagret, och eliminerar behovet av ett routingprotokoll som hanterar flera hopp.

Den dåliga prestandan hos TCP har gjort User Datagram Protocol, UDP, till standardvalet för transportprotokoll i LLN-tillämpningar. Datagram Transport Layer Security, DTLS, är ett UDP-baserad protokoll för säker kommunikation, vidareutvecklat från det TCP-baserade Transport Layer Security, TLS.

Att skapa en session för säker kommunikation i DTLS kräver intensivt kommunikation, med betydande extra kostnader på grund av stora meddelanden och resulterande fragmentering av IP-paketen. I denna avhandling introducerar vi nya mekanismer för att komprimera protokolldata och minska storleken på DTLS-meddelanden, utan att bryta säkerheten mellan ändpunkterna. Att minska storleken på DTLS-meddelanden minskar mängden overhead för kommunikationen, och undviker fragmentering av IP-paket.

Glossy är inte designat som ett säkerhetsprotokoll. Därför är Glossy som ett LLN-protokoll känsligt för obehörig avlyssning och attacker som stör ordinarie nätverkstrafik. I denna avhandling studerar vi effektiviteten hos ett antal attacker som syftar till att störa de synkroniserade sändningar som Glossy använder. Utifrån resultaten av studierna bedömer vi säkerhetskraven för protokoll som bygger på Glossy. Vi föreslår kryptering, resurseffektiv verifiering av flooding-operationer och autentiserade metoder för schemauppdateringar, för att skydda Glossy-baserade protokoll som LWB.

Optical Wireless Communication, OWC, har trätt fram som en kompletterande teknik till radiobaserad kommunikation. Till skillnad från radiospektrumet är de optiska frekvenserna till största delen oreglerade, och säkra att använda i miljöer som är känsliga för elektromagnetisk störning. På grund av begränsad räckvidd så har en rad OWC-system för att hantera multi-hopp föreslagits, motiverade av meshrouting-protokoll för LLN. Synkroniserade överföringar inom radionätverk har studerats noggrant, men inga sådana studier har gjorts för OWC. Inspirerat av Glossy presenterar vi designen av ett nytt system för OWC-baserad tidssynkronisering, som utnyttjar kommunikation med infrarött ljus. Målet är en OWC-baserad tjänst som låter ändpunkter schemalägga sin kommunikation.

Genom denna avhandling undersöker jag utvalda forskningsfrågor om prestandaförbättringar och säkerhetsaspekter för IoT-protokoll. Uppföljande studier av andra forskare har visat på flera tänkbara alternativ, vilket visar på behovet av mer undersökningar. Oavsett så är jag övertygad om att insikterna som presenteras i denna avhandling kommer att vara till hjälp för fortsatt forskning inom LLN och göra nya vägar inom OWC möjliga.

References

[1] Lars Almon, Michael Riecker, and Matthias Hollick. "Lightweight Detection of Denial-of-Service Attacks on Wireless Sensor Networks Revisited". In: *2017 IEEE 42nd Conference on Local Computer Networks (LCN)*. 2017, pp. 444–452. DOI: 10.1109/LCN.2017.110.

[2] Yasmin M. Amin and Amr T. Abdel-Hamid. "A Comprehensive Taxonomy and Analysis of IEEE 802.15.4 Attacks". In: *JECE* 2016 (2016), p. 4. DOI: 10.1155/2016/7165952.

[3] Farhana Ashraf, Yih-Chun Hu, and Robin H. Kravets. "Bankrupting the jammer in WSN". In: *2012 IEEE 9th International Conference on Mobile Ad-Hoc and Sensor Systems (MASS 2012)*. 2012, pp. 317–325. DOI: 10.1109/MASS.2012.6502531.

[4] Emmanuel Baccelli, Oliver Hahm, Mesut Günes, Matthias Wählisch, and Thomas C. Schmidt. "RIOT OS: Towards an OS for the Internet of Things". In: *2013 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. 2013, pp. 79–80. DOI: 10.1109/INFCOMW.2013.6970748.

[5] Utsav Banerjee, Chiraag Juvekar, Samuel H. Fuller, and Anantha P. Chandrakasan. "eeDTLS: Energy-Efficient Datagram Transport Layer Security for the Internet of Things". In: *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*. 2017, pp. 1–6. DOI: 10.1109/GLOCOM.2017.8255053.

[6] Simon Bauer, Benedikt Jaeger, Fabian Helfert, Philippe Barias, and Georg Carle. "On the Evolution of Internet Flow Characteristics". In: *Proceedings of the Applied Networking Research Workshop*. ANRW '21. Association for Computing Machinery, 2021, pp. 29–35. DOI: 10.1145/3472305.3472321.

[7] Balkis Bettoumi and Ridha Bouallegue. "LC-DEX: Lightweight and Efficient Compressed Authentication Based Elliptic Curve Cryptography in Multi-Hop 6LoWPAN Wireless Sensor Networks in HIP-Based Internet of Things". In: *Sensors* 21.21 (2021). DOI: 10.3390/s21217348.

[8] August Betzler, Carles Gomez, Ilker Demirkol, and Josep Paradells. "CoAP congestion control for the internet of things". In: *IEEE Communications Magazine* 54.7 (2016), pp. 154–160. DOI: 10.1109/MCOM.2016.7509394.

[9] Carlo Alberto Boano, Markus Schuß, and Kay Römer. *EWSN Dependability Competition: Experiences and Lessons Learned*. Web page: `https://iot.ieee.org/newsletter/march-2017/ewsn-dependability-competition-experiences-and-lessons-learned`. Visited 2023-05-10. 2017.

[10] Kai Lennert Bober, Eric Ackermann, Ronald Freund, Volker Jungnickel, Tuncer Baykas, and Sang-Kyu Lim. "The IEEE 802.15.13 Standard for Optical Wireless Communications in Industry 4.0". In: *IECON 2022 - 48th Annual Conference of the IEEE Industrial Electronics Society*. 2022, pp. 1–6. DOI: `10.1109/IECON49645.2022.9968724`.

[11] Carsten Bormann. *6LoWPAN-GHC: Generic Header Compression for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)*. RFC 7400. 2014. DOI: `10.17487/RFC7400`.

[12] Rachid Bouziane and Robert Killey. "Blind symbol synchronization for direct detection optical OFDM using a reduced number of virtual subcarriers". In: *Optics Express* 23.5 (2015), pp. 6444–6454. DOI: `10.1364/OE.23.006444`.

[13] Martina Brachmann, Olaf Landsiedel, and Silvia Santini. "Concurrent Transmissions for Communication Protocols in the Internet of Things". In: *2016 IEEE 41st Conference on Local Computer Networks (LCN)*. 2016, pp. 406–414. DOI: `10.1109/LCN.2016.69`.

[14] Torsten Braun, Thiemo Voigt, and Adam Dunkels. "TCP support for sensor networks". In: *2007 Fourth Annual Conference on Wireless on Demand Network Systems and Services*. 2007, pp. 162–169. DOI: `10.1109/WONS.2007.340494`.

[15] Harald Burchardt, Nikola Serafimovski, Dobroslav Tsonev, Stefan Videv, and Harald Haas. "VLC: Beyond point-to-point communication". In: *IEEE Communications Magazine* 52.7 (2014), pp. 98–105. DOI: `10.1109/MCOM.2014.6852089`.

[16] Xianghui Cao, Devu Manikantan Shila, Yu Cheng, Zequ Yang, Yang Zhou, and Jiming Chen. "Ghost-in-ZigBee: Energy Depletion Attack on ZigBee-Based Wireless Networks". In: *IEEE Internet of Things Journal* 3.5 (2016), pp. 816–829. DOI: `10.1109/JIOT.2016.2516102`.

[17] Tengfei Chang, Thomas Watteyne, Xavier Vilajosana, and Pedro Henrique Gomes. "Constructive Interference in 802.15.4: A Tutorial". In: *IEEE Communications Surveys & Tutorials* 21.1 (2019), pp. 217–237. DOI: `10.1109/COMST.2018.2870643`.

[18] Helal Chowdhury and Marcos Katz. "Cooperative multihop connectivity performance in visible light communications". In: *2013 IFIP Wireless Days (WD)*. 2013, pp. 1–4. DOI: `10.1109/WD.2013.6686444`.

[19] Hyunchae Chun, Ariel Gomez, Crisanto Quintana, Weida Zhang, Grahame Faulkner, and Dominic O'Brien. "A Wide-Area Coverage 35 Gb/s Visible Light Communications Link for Indoor Wireless Applications". In: *Scientific reports* 9.1 (2019), p. 4952. DOI: 10.1038/s41598-019-41397-6.

[20] Moteiv Corporation. *Tmote Sky*. Web page: https://www.snm.ethz.ch/snmwiki/Projects/TmoteSky.html. Visited 2023-05-15.

[21] Yuanbo Deng and Daping Chu. "Coherence properties of different light sources and their effect on the image sharpness and speckle of holographic displays". In: *Scientific Reports* 7 (2017). DOI: 10.1038/s41598-017-06215-x.

[22] Wan Du, Jansen Christian Liando, Huanle Zhang, and Mo Li. "Pando: Fountain-Enabled Fast Data Dissemination With Constructive Interference". In: *IEEE/ACM Transactions on Networking* 25.2 (2017), pp. 820–833. DOI: 10.1109/TNET.2016.2614707.

[23] Adam Dunkels. "Full TCP/IP for 8-Bit Architectures". In: *Proceedings of the 1st International Conference on Mobile Systems, Applications and Services*. MobiSys '03. Association for Computing Machinery, 2003, pp. 85–98.

[24] Adam Dunkels, Juan Alonso, Thiemo Voigt, and Hartmut Ritter. *Distributed TCP caching for wireless sensor networks*. 2004.

[25] Adam Dunkels, Juan Alonso, Thiemo Voigt, Hartmut Ritter, and Jochen Schiller. "Connecting Wireless Sensornets with TCP/IP Networks". In: *Wired/Wireless Internet Communications*. Springer Berlin Heidelberg, 2004, pp. 143–152. DOI: 10.1007/978-3-540-24643-5_13.

[26] Simon Duquennoy, Fredrik Österlind, and Adam Dunkels. "Lossy Links, Low Power, High Throughput". In: *Proceedings of the 9th ACM Conference on Embedded Networked Sensor Systems*. SenSys '11. Association for Computing Machinery, 2011, pp. 12–25. DOI: 10.1145/2070942.2070945.

[27] 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*. SenSys '12. Association for Computing Machinery, 2012, pp. 1–14. DOI: 10.1145/2426656.2426658.

[28] 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*. 2011, pp. 73–84.

[29] Linux Foundation and Wind River Systems. *Zephyr Project*. Web page: https://www.zephyrproject.org. Visited 2023-05-10. 2023.

[30] Alexandros Fragkiadakis. “DTLS Static Context Header Compression -Implementation and Evaluation in the Contiki-NG”. In: *2022 IEEE Conference on Standards for Communications and Networking (CSCN)*. 2022, pp. 131–137. doi: 10.1109/CSCN57023.2022.10051055.

[31] XiangFa Guo, Mobashir Mohammad, Sudipta Saha, Mun Choon Chan, Seth Gilbert, and Derek Leong. “PSync: Visible light-based time synchronization for Internet of Things (IoT)”. In: *IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications*. 2016, pp. 1–9. doi: 10.1109/INFOCOM.2016.7524358.

[32] 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)*. 2016, pp. 1–9. doi: 10.1109/SAHCN.2016.7732971.

[33] 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*. 2013, pp. 542–550. doi: 10.1109/MASS.2013.18.

[34] Tor Helleseth. “De Bruijn Sequence”. In: *Encyclopedia of Cryptography and Security*. Ed. by Henk C. A. van Tilborg and Sushil Jajodia. Springer US, 2011, pp. 315–316. doi: 10.1007/978-1-4419-5906-5_344.

[35] Joel Höglund, Samuel Lindemer, Martin Furuhed, and Shahid Raza. “PKI4IoT: Towards public key infrastructure for the Internet of Things”. In: *Computers & Security (Elsevier)* 89 (2020), p. 101658. doi: 10.1016/j.cose.2019.101658.

[36] Mahmud Hossain, Yasser Karim, and Ragib Hasan. “SecuPAN: A Security Scheme to Mitigate Fragmentation-Based Network Attacks in 6LoWPAN”. In: *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy*. CODASPY ’18. Association for Computing Machinery, 2018, pp. 307–318. doi: 10.1145/3176258.3176326.

[37] Mahmud Hossain, Golam Kayas, Yasser Karim, Ragib Hasan, Jamie Payton, and S. M. Riazul Islam. “CATComp: A Compression-Aware Authorization Protocol for Resource-Efficient Communications in IoT Networks”. In: *IEEE Internet of Things Journal* 9.3 (2022), pp. 1667–1682. doi: 10.1109/JIOT.2021.3092183.

[38] Ding-Jie Huang, Kai-Jie You, and Wei-Chung Teng. “Secured Flooding Time Synchronization Protocol”. In: *2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems*. 2011, pp. 620–625. doi: 10.1109/MASS.2011.64.

[39] René Hummen, Jens Hiller, Martin Henze, and Klaus Wehrle. “Slimfit - A HIP DEX compression layer for the IP-based Internet of Things”. In: *2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. 2013, pp. 259–266. DOI: 10.1109/WiMOB.2013.6673370.

[40] René Hummen, Jens Hiller, Hanno Wirtz, Martin Henze, Hossein Shafagh, and Klaus Wehrle. “6LoWPAN Fragmentation Attacks and Mitigation Mechanisms”. In: *Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks*. WiSec ’13. Association for Computing Machinery, 2013, pp. 55–66. DOI: 10.1145/2462096.2462107.

[41] Philipp Hurni, Ulrich Bürgi, Markus Anwander, and Torsten Braun. “TCP Performance Optimizations for Wireless Sensor Networks”. In: *Wireless Sensor Networks*. Springer Berlin Heidelberg, 2012, pp. 17–32. DOI: 10.1007/978-3-642-28169-3_2.

[42] “IEEE Approved Draft Standard for Multi-Gigabit per Second Optical Wireless Communications (OWC), with Ranges up to 200 meters, for both stationary and mobile devices”. In: *IEEE P802.15.13/D10.0, November 2022* (2023), pp. 1–154.

[43] “IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems”. In: *IEEE Std 1588-2019 (Revision ofIEEE Std 1588-2008)* (2020), pp. 1–499. DOI: 10.1109/IEEESTD.2020.9120376.

[44] “IEEE Standard for Low-Rate Wireless Networks”. In: *IEEE Std 802.15.4-2020 (Revision of IEEE Std 802.15.4-2015)* (2020), pp. 1–800. DOI: 10.1109/IEEESTD.2020.9144691.

[45] Oana Iova, Pietro Picco, Timofei Istomin, and Csaba Kiraly. “RPL: The Routing Standard for the Internet of Things... Or Is It?” In: *IEEE Communications Magazine* 54.12 (2016), pp. 16–22. DOI: 10.1109/MCOM.2016.1600397CM.

[46] Timofei Istomin, Amy L. Murphy, Gian Pietro Picco, and Usman Raza. “Data Prediction + Synchronous Transmissions = Ultra-Low Power Wireless Sensor Networks”. In: *Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM*. SenSys ’16. Association for Computing Machinery, 2016, pp. 83–95. DOI: 10.1145/2994551.2994558.

[47] Yogesh G. Iyer, Shashidhar Gandham, and Subbarayan Venkatesan. “STCP: a generic transport layer protocol for wireless sensor networks”. In: *Proceedings. 14th International Conference on Computer Communications and Networks, 2005. ICCCN 2005.* 2005, pp. 449–454. DOI: 10.1109/ICCCN.2005.1523908.

[48] Jithin Jagannath and Tommaso Melodia. “An Opportunistic Medium Access Control Protocol for Visible Light Ad Hoc Networks”. In: *2018 International Conference on Computing, Networking and Communications (ICNC)*. 2018, pp. 609–614. DOI: 10.1109/ICCNC.2018.8390277.

[49] Jithin Jagannath and Tommaso Melodia. “VL-ROUTE: A Cross-Layer Routing Protocol for Visible Light Ad Hoc Network”. In: *2019 IEEE 20th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*. 2019, pp. 1–9. DOI: 10.1109/WoWMoM.2019.8793030.

[50] Hyung-Sin Kim, Heesu Im, Myung-Sup Lee, Jeongyeup Paek, and Saewoong Bahk. “A measurement study of TCP over RPL in low-power and lossy networks”. In: *Journal of Communications and Networks* 17.6 (2015), pp. 647–655. DOI: 10.1109/JCN.2015.000111.

[51] Lennart Klaver and Marco Zuniga. “Shine: A Step Towards Distributed Multi-Hop Visible Light Communication”. In: *2015 IEEE 12th International Conference on Mobile Ad Hoc and Sensor Systems*. 2015, pp. 235–243. DOI: 10.1109/MASS.2015.78.

[52] Sam Kumar, Michael P Andersen, Hyung-Sin Kim, and David E. Culler. “Performant TCP for Low-Power Wireless Networks”. In: *17th USENIX Symposium on Networked Systems Design and Implementation (NSDI 20)*. Santa Clara, CA: USENIX Association, 2020, pp. 911–932.

[53] Hyuksang Kwon, Jeongseob Ahn, and JeongGil Ko. “LightCert: On designing a lighter certificate for resource-limited Internet-of-Things devices”. In: *Transactions on Emerging Telecommunications Technologies* 30.10 (2019). DOI: 10.1002/ett.3740.

[54] Krijn Leentvaar and Jan H. Flint. “The Capture Effect in FM Receivers”. In: *IEEE Transactions on Communications* 24.5 (1976), pp. 531–539.

[55] Chansook Lim. “Improving Congestion Control of TCP for Constrained IoT Networks”. In: *MDPI Sensors* 20.17 (2020). DOI: 10.3390/s20174774.

[56] 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. DOI: 10.1145/2461381.2461402.

[57] Charles Lockie, Ioannis Mavromatis, Aleksandar Stanoev, Yichao Jin, and George Oikonomou. “Securing Synchronous Flooding Communications: An Atomic-SDN Implementation”. In: *Proceedings of the 2022 International Conference on Embedded Wireless Systems and Networks*. EWSN ’22. Association for Computing Machinery, 2023, pp. 250–255.

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

[59] Lukas Bereuter, Mirco Gysin, Thomas Kueffer, Martin Kucera, Thomas Niederhauser, Jürg Fuhrer, Paul Heinisch, Adrian Zurbuchen, Dominik Obrist, Hildegard Tanner, and Andreas Haeberlin. “Leadless Dual-Chamber Pacing: A Novel Communication Method for Wireless Pacemaker Synchronization”. In: *JACC: Basic to Translational Science* 3.6 (2018), pp. 813–823. DOI: 10.1016/j.jacbts.2018.07.009.

[60] Miklós Maróti, Branislav Kusy, Gyula Simon, and Ákos Lédeczi. “The Flooding Time Synchronization Protocol”. In: *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems*. SenSys ’04. Association for Computing Machinery, 2004, pp. 39–49. DOI: 10.1145/1031495.1031501.

[61] Jim Martin, Jack Burbank, William Kasch, and Professor David L. Mills. *Network Time Protocol Version 4: Protocol and Algorithms Specification*. RFC 5905. 2010. DOI: 10.17487/RFC5905.

[62] Luiz Eduardo Mendes Matheus, Alex Borges Vieira, Luiz F. M. Vieira, Marcos A. M. Vieira, and Omprakash Gnawali. “Visible Light Communication: Concepts, Applications and Challenges”. In: *IEEE Communications Surveys & Tutorials* 21.4 (2019), pp. 3204–3237. DOI: 10.1109/COMST.2019.2913348.

[63] Michael Baddeley, Carlo Alberto Boano, Antonio Escobar-Molero, Ye Liu, Xiaoyuan Ma, Victor Marot, Usman Raza, Kay Römer, Markus Schuß, and Aleksandar Stanoev. “Understanding Concurrent Transmissions”. In: *ACM Transactions on Sensor Networks* (2023). DOI: 10.1145/3604430.

[64] Ana Minaburo, Laurent Toutain, and Ricardo Andreasen. *Static Context Header Compression (SCHC) for the Constrained Application Protocol (CoAP)*. RFC 8824. 2021. DOI: 10.17487/RFC8824.

[65] Robert Moskowitz, Tobias Heer, Petri Jokela, and Thomas R. Henderson. *Host Identity Protocol Version 2 (HIPv2)*. RFC 7401. 2015. DOI: 10.17487/RFC7401.

[66] Omer Narmanlioglu, Refik Caglar Kizilirmak, Farshad Miramirkhani, and Murat Uysal. “Cooperative Visible Light Communications With Full-Duplex Relaying”. In: *IEEE Photonics Journal* 9.3 (2017), pp. 1–11. DOI: 10.1109/JPHOT.2017.2708746.

[67] George Oikonomou, Simon Duquennoy, Atis Elsts, Joakim Eriksson, Yasuyuki Tanaka, and Nicolas Tsiftes. “The Contiki-NG open source operating system for next generation IoT devices”. In: *SoftwareX* 18 (2022), p. 101089. DOI: 10.1016/j.softx.2022.101089.

[68] Jonathan Oostvogels, Fan Yang, Sam Michiels, and Danny Hughes. “Zero-Wire: A Deterministic and Low-Latency Wireless Bus through Symbol-Synchronous Transmission of Optical Signals”. In: *Proceedings of the 18th Conference on Embedded Networked Sensor Systems*. SenSys ’20. New York, NY, USA: Association for Computing Machinery, 2020, pp. 164–178. DOI: 10.1145/3384419.3430897.

[69] Jeongyeup Paek and Ramesh Govindan. “RCRT: Rate-Controlled Reliable Transport for Wireless Sensor Networks”. In: *Proceedings of the 5th International Conference on Embedded Networked Sensor Systems*. SenSys ’07. Association for Computing Machinery, 2007, pp. 305–319. DOI: 10.1145/1322263.1322293.

[70] Qixiang Pang and Vincent Wong. “Reliable data transport and congestion control in wireless sensor networks”. In: *International Journal of Sensor Networks* 3 (2008), pp. 16–24. DOI: 10.1504/IJSNET.2008.016458.

[71] Mingyu Park and Jeongyeup Paek. “TAiM: TCP assistant-in-the-middle for multihop low-power and lossy networks in IoT”. In: *Journal of Communications and Networks* 21.2 (2019), pp. 192–199. DOI: 10.1109/JCN.2019.000017.

[72] Mingyu Park and Jeongyeup Paek. “TAiM: TCP assistant-in-the-middle for multihop low-power and lossy networks in IoT”. In: *Journal of Communications and Networks* 21.2 (2019), pp. 192–199. DOI: 10.1109/JCN.2019.000017.

[73] Christina Popper, Mario Strasser, and Srdjan Capkun. “Anti-jamming broadcast communication using uncoordinated spread spectrum techniques”. In: *IEEE Journal on Selected Areas in Communications* 28.5 (2010), pp. 703–715. DOI: 10.1109/JSAC.2010.100608.

[74] pureLiFi. *LiFi-XC™: Fully networked wireless communications system for the evaluation of LiFi use cases*. Web page: https://www.purelifi.com/products/lifi-xc. Visited 2023-05-10. 2023.

[75] Tie Qiu, Xize Liu, Min Han, Huansheng Ning, and Dapeng Oliver Wu. “A Secure Time Synchronization Protocol Against Fake Timestamps for Large-Scale Internet of Things”. In: *IEEE Internet of Things Journal* 4.6 (2017), pp. 1879–1889. DOI: 10.1109/JIOT.2017.2714904.

[76] Michael Rahaim and Thomas D. C. Little. “Interference in IM/DD optical wireless communication networks”. In: *Journal of Optical Communications and Networking* 9.9 (2017), pp. D51–D63. DOI: 10.1364/JOCN.9.000D51.

[77] Shahid Raza, Simon Duquennoy, Tony Chung, Dogan Yazar, Thiemo Voigt, and Utz Roedig. “Securing communication in 6LoWPAN with compressed IPsec”. In: *2011 International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS)*. 2011, pp. 1–8. DOI: 10.1109/DCOSS.2011.5982177.

[78] Eric Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.3*. RFC 8446. 2018. DOI: 10.17487/RFC8446.

[79] Eric Rescorla, Richard Barnes, Hannes Tschofenig, and Benjamin M. Schwartz. *Compact TLS 1.3*. Internet-Draft draft-ietf-tls-ctls-08. Work in Progress. Internet Engineering Task Force, 2023. 24 pp.

[80] Eric Rescorla and Nagendra Modadugu. *Datagram Transport Layer Security Version 1.2*. RFC 6347. 2012. DOI: 10.17487/RFC6347.

[81] Eric Rescorla, Hannes Tschofenig, and Nagendra Modadugu. *The Datagram Transport Layer Security (DTLS) Protocol Version 1.3*. RFC 9147. 2022. DOI: 10.17487/RFC9147.

[82] Michael Riecker, Daniel Thies, and Matthias Hollick. “Measuring the impact of denial-of-service attacks on wireless sensor networks”. In: *39th Annual IEEE Conference on Local Computer Networks*. 2014, pp. 296–304. DOI: 10.1109/LCN.2014.6925784.

[83] Tanya Roosta, Wei-Chieh Liao, Wei-Chung Teng, and Shankar Sastry. “Testbed Implementation of a Secure Flooding Time Synchronization Protocol”. In: *2008 IEEE Wireless Communications and Networking Conference*. 2008, pp. 3157–3162. DOI: 10.1109/WCNC.2008.551.

[84] Somia Sahraoui and Azeddine Bilami. “Efficient HIP-based approach to ensure lightweight end-to-end security in the internet of things”. In: *Computer Networks* 91 (2015), pp. 26–45. DOI: 10.1016/j.comnet.2015.08.002.

[85] Matt Sargent, Jerry Chu, Dr. Vern Paxson, and Mark Allman. *Computing TCP’s Retransmission Timer*. RFC 6298. 2011. DOI: 10.17487/RFC6298.

[86] Stefan Schmid, Thomas Richner, Stefan Mangold, and Thomas R. Gross. “EnLighting: An Indoor Visible Light Communication System Based on Networked Light Bulbs”. In: *2016 13th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*. 2016, pp. 1–9. DOI: 10.1109/SAHCN.2016.7732989.

[87] Zach Shelby, Klaus Hartke, and Carsten Bormann. *The Constrained Application Protocol (CoAP)*. RFC 7252. 2014. DOI: 10.17487/RFC7252.

[88] Michael Spuhler, Domenico Giustiniano, Vincent Lenders, Matthias Wilhelm, and Jens B. Schmitt. “Detection of Reactive Jamming in DSSS-based Wireless Communications”. In: *IEEE Transactions on Wireless Communications* 13.3 (2014), pp. 1593–1603. DOI: 10.1109/TWC.2013.013014.131037.

[89] Mario Strasser, Boris Danev, and Srdjan Čapkun. “Detection of Reactive Jamming in Sensor Networks”. In: *ACM Trans. Sen. Netw.* 7.2 (2010). DOI: 10.1145/1824766.1824772.

[90] RIOT Operating System. *Generic (GNRC) network stack*. Web page: https://doc.riot-os.org/group__net__gnrc.html. Visited 2023-05-10. 2023.

[91] Pascal Thubert and Jonathan Hui. *Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks*. RFC 6282. 2011. DOI: 10.17487/RFC6282.

[92] Máté Tömösközi, Martin Reisslein, and Frank H. P. Fitzek. “Packet Header Compression: A Principle-Based Survey of Standards and Recent Research Studies”. In: *IEEE Communications Surveys & Tutorials* 24.1 (2022), pp. 698–740. DOI: 10.1109/COMST.2022.3144473.

[93] Cheng-Xiang Wang et al. “On the Road to 6G: Visions, Requirements, Key Technologies, and Testbeds”. In: *IEEE Communications Surveys & Tutorials* 25.2 (2023), pp. 905–974. DOI: 10.1109/COMST.2023.3249835.

[94] Liang-Yu Wei, Yang Liu, Chi-Wai Chow, Guan-Hong Chen, Ching-Wei Peng, Pin-Cheng Guo, Jui-Feng Tsai, and Chien-Hung Yeh. “6.915-Gbit/s white-light phosphor laser diode-based DCO-OFDM visible light communication (VLC) system with functional transmission distance”. In: *Electronics Letters* 56.18 (2020), pp. 945–947. DOI: 10.1049/el.2020.1379.

[95] Hongming Yang and Ashish Pandharipande. “Full-duplex relay VLC in LED lighting linear system topology”. In: *IECON 2013 - 39th Annual Conference of the IEEE Industrial Electronics Society*. 2013, pp. 6075–6080. DOI: 10.1109/IECON.2013.6700133.

[96] Yuliang Li, Gautam Kumar, Hema Hariharan, Hassan Wassel, Peter Hochschild, Dave Platt, Simon Sabato, Minlan Yu, Nandita Dukkipati, Prashant Chandra, and Amin Vahdat. “Sundial: Fault-tolerant Clock Synchronization for Datacenters”. In: *14th USENIX Symposium on Operating Systems Design and Implementation (OSDI 20)*. USENIX Association, 2020, pp. 1171–1186.

[97] Chao Zhang, Jia Ye, Gaofeng Pan, and Zhiguo Ding. “Cooperative Hybrid VLC-RF Systems With Spatially Random Terminals”. In: *IEEE Transactions on Communications* 66.12 (2018), pp. 6396–6408. DOI: `10.1109/TCOMM.2018.2865949`.

[98] 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* 53.6 (2020). DOI: `10.1145/3410159`.

[99] Zolertia. *Firefly*. Web page: `https://github.com/Zolertia/Resources`. Visited 2023-05-15.

Acta Universitatis Upsaliensis

Digital Comprehensive Summaries of Uppsala Dissertations from the Faculty of Science and Technology 2283

Editor: The Dean of the Faculty of Science and Technology

ACTA UNIVERSITATIS
UPSALIENSIS
2023

Distribution: publications.uu.se
urn:nbn:se:uu:diva-506085