Mälardalen University Press Dissertations
No. 139

LIGHTWEIGHT SECURITY SOLUTIONS FOR THE INTERNET OF THINGS

Shahid Raza

2013

School of Innovation, Design and Engineering

ISBN 978-91-7485-110-6
ISSN 1651-4238
Printed by Mälardalen University, Västerås, Sweden

Mälardalen University Press Dissertations
No. 139

LIGHTWEIGHT SECURITY SOLUTIONS FOR THE INTERNET OF THINGS

Shahid Raza

Akademisk avhandling

som för avläggande av teknologie doktorsexamen i datavetenskap vid
Akademin för innovation, design och teknik kommer att offentligen försvaras
onsdagen den 5 juni 2013, 10.15 i Kappa, Mälardalens högskola, Västerås.

Fakultetsopponent: Adjunct Associate Professor Wen Hu, University of New South Wales

Akademin för innovation, design och teknik

Abstract

The future Internet will be an IPv6 network interconnecting traditional computers and a large number of smart object or networks such as Wireless Sensor Networks (WSNs). This Internet of Things (IoT) will be the foundation of many services and our daily life will depend on its availability and reliable operations.

Therefore, among many other issues, the challenge of implementing secure communication in the IoT must be addressed. The traditional Internet has established and tested ways of securing networks. The IoT is a hybrid network of the Internet and resource-constrained networks, and it is therefore reasonable to explore the options of using security mechanisms standardized for the Internet in the IoT.

The IoT requires multi-facet security solutions where the communication is secured with confidentiality, integrity, and authentication services; the network is protected against intrusions and disruptions; and the data inside a sensor node is stored in an encrypted form. Using standardized mechanisms, communication in the IoT can be secured at different layers: at the link layer with IEEE 802.15.4 security, at the network layer with IP security (IPsec), and at the transport layer with Datagram Transport Layer Security (DTLS). Even when the IoT is secured with encryption and authentication, sensor nodes are exposed to wireless attacks both from inside the WSN and from the Internet. Hence an Intrusion Detection System (IDS) and firewalls are needed. Since the nodes inside WSNs can be captured and cloned, protection of stored data is also important.

This thesis has three main contributions. (i) It enables secure communication in the IoT using lightweight compressed yet standard compliant IPsec, DTLS, and IEEE 802.15.4 link layer security; and it discusses the pros and cons of each of these solutions. The proposed security solutions are implemented and evaluated in an IoT setup on real hardware. (ii) This thesis also presents the design, implementation, and evaluation of a novel IDS for the IoT. (iii) Last but not least, it also provides mechanisms to protect data inside constrained nodes.

The experimental evaluation of the different solutions shows that the resource-constrained devices in the IoT can be secured with IPsec, DTLS, and 802.15.4 security; can be efficiently protected against intrusions; and the proposed combined secure storage and communication mechanisms can significantly reduce the security-related operations and energy consumption.

ISBN 978-91-7485-110-6
ISSN 1651-4238

Swedish Institute of Computer Science
Doctoral Thesis
SICS Dissertation Series 64

Lightweight Security Solutions for the Internet of Things

Shahid Raza

2013

Swedish Institute of Computer Science(SICS)
SICS Swedish ICT, Kista
Stockholm, Sweden

ISSN 1101-1335
ISRN SICS-D–64–SE
Printed by Mälardalen University, Västerås, Sweden

Abstract

The future Internet will be an IPv6 network interconnecting traditional computers and a large number of smart objects or networks such as Wireless Sensor Networks (WSNs). This Internet of Things (IoT) will be the foundation of many services and our daily life will depend on its availability and reliable operations. Therefore, among many other issues, the challenge of implementing secure communication in the IoT must be addressed. The traditional Internet has established and tested ways of securing networks. The IoT is a hybrid network of the Internet and resource-constrained networks, and it is therefore reasonable to explore the options of using security mechanisms standardized for the Internet in the IoT.

The IoT requires multi-faceted security solutions where the communication is secured with confidentiality, integrity, and authentication services; the network is protected against intrusions and disruptions; and the data inside a sensor node is stored in an encrypted form. Using standardized mechanisms, communication in the IoT can be secured at different layers: at the link layer with IEEE 802.15.4 security, at the network layer with IP security (IPsec), and at the transport layer with Datagram Transport Layer Security (DTLS). Even when the IoT is secured with encryption and authentication, sensor nodes are exposed to wireless attacks both from inside the WSN and from the Internet. Hence an Intrusion Detection System (IDS) and firewalls are needed. Since the nodes inside WSNs can be captured and cloned, protection of stored data is also important.

This thesis has three main contributions. (i) It enables secure communication in the IoT using lightweight compressed yet standard compliant IPsec, DTLS, and IEEE 802.15.4 link layer security; and it discusses the pros and cons of each of these solutions. The proposed security solutions are implemented and evaluated in an IoT setup on real hardware. (ii) This thesis also presents the design, implementation, and evaluation of a novel IDS for the IoT. (iii) Last but

not least, it also provides mechanisms to protect data inside constrained nodes. The experimental evaluation of the different solutions shows that the resource-constrained devices in the IoT can be secured with IPsec, DTLS, and 802.15.4 security; can be efficiently protected against intrusions; and the proposed combined secure storage and communication mechanisms can significantly reduce the security-related operations and energy consumption.

Sammanfattning

Framtidens Internet är ett IPv6-nätverk vilket förbinder traditionella datorer och ett stort antal smarta objekt eller nätverk som trådlösa sensornätverk (WSN). Detta Internet of Things (IoT) kommer att vara grunden för många tjänster och vårt dagliga liv kommer att bero pådess tillgänglighet och säkra drift. Därför måste man bland många andra frågor adressera utmaningen att skapa säker kommunikation i Internet of Things. Det traditionella Internet har etablerat och testat olika sätt att skapa säkra nätverk. IoT är en blandning av nätverk, av Internet och nät med småresurser, och det är därför viktigt att undersöka möjligheterna att använda säkerhetsmekanismer standardiserade för Internet i Internet of Things.

Internet of Things kräver mångfacetterade säkerhetslösningar där kommunikationen är säkrad med sekretess, integritet och autentisering av tjänster, nätverket skyddas mot intrång och störningar, och data inuti en sensornod lagras i krypterad form. Med standardiserade mekanismer kan kommunikationen säkras i olika skikt: i länkskiktet med IEEE 802.15.4-säkerhet, i nätskiktet med IP-säkerhet (IPsec), och i transportskiktet med Datagram Transport Layer Security (DTLS) . ven när kommunikationen är säkrad med kryptering och autentisering är sensornoderna utsatta både för trådlösa attacker inifrån WSN och från Internet. Därför behövs ett system för att upptäcka intrång (Intrusion Detection System, IDS), och även brandväggar behövs. Eftersom noderna inne i WSN kan stjälas och klonas, är skyddet av lagrade data också viktigt.

Denna avhandling har tre huvudsakliga bidrag. (i) Den möjliggör säker kommunikation i Internet of Things med lättviktiga, komprimerade, men standardkompatibla IPsec, DTLS och IEEE 802.15.4-länkskiktssäkerhet, och jämför för- och nackdelar mellan dessa lösningar. De föreslagna säkerhetslösningarna implementeras och utvärderas i en IoT-installation påriktig hårdvara. (ii) Denna avhandling presenterar också design, implementation och utvärdering av ett nytt IDS för Internet of Things. (iii) Sist men inte minst, avhandlingen pre-

senterar ocksåmekanismer för att skydda data i noder med begränsade resurser. Den kvantitativa utvärderingen av de olika lösningarna visar att enheter i IoT med begränsade resurser kan säkras med IPsec, DTLS och 802.15.4-säkerhet, och kan effektivt skyddas mot intrång, och den föreslagna kombinationen av säker lagring och mekanismer för säker kommunikation kan avsevärt minska kostanden för säkerhetsrelaterade operationer och energiförbrukning.

Acknowledgements

First and foremost, I am thankful to Almighty Allah for bestowing me health, persistence, and knowledge to complete this work. I implore Him to make my knowledge and skills useful to mankind.

I am obliged to all the people in SICS Swedish ICT, Mälardalen University, and ABB who were associated with this work and guided me throughout the thesis period, but it is worth mentioning some of the people who were really benevolent and supportive. I first express my gratitude to my advisor Prof. Thiemo Voigt for his unprecedented support, extensive guidance, and personal involvement in all phases of this research. Without his encouragement, guidance, and keen interest this thesis would not have been completed.

I am deeply indebted and grateful to my supervisors Prof. Mats Björkman, Dr. Christian Gehrmann, Prof. Seif Haridi, and Thiemo Voigt for providing me the much needed motivation, inspiration and guidance in achieving this milestone. Its been pleasure to work with the co-authors around the globe. I genuinely thank Utz Roedig, Ibrahim Ethem Bagci, and Tony Chung from Lancaster University; Krister Landernäs and Mikael Gidlund for ABB; Gianluca Dini from University of Pisa; Kasun from Uppsala University; René Hummen from RWTH Aachen University; and Adriaan, Dogan, Hossein, Joel, Linus, Simon, and Thiemo from SICS.

I am very grateful to Dr. Sverker Janson, head of the Computer Systems Laboratory (CSL) and a supportive mentor, for helping me in all academic and non-academic matters whenever needed. I am thankful to my current and formers co-workers in NES group: Adriaan, Adam, Beshr, Dogan, Fredrik, Joakim, Joel, Luca, Niclas, Nicolas, Niklas, Prasant, Zhitao, and obviously Simon and Thiemo. I acknowledge all colleagues at SICS particularly Mudassar Aslam, Eva Gudmundsson, Jerker Berg, Thomas Ringström, Lotta Jörsäter, Karin Fohlstedt, Vicki Knopf, Bengt Ahlgren, Maria Holm, Oliver Schwarz, Orc Lönn, Rolf Blom, and of course Janusz Launberg and Christer Norström.

Last, but certainly not least, I cannot thank my family enough for the unend-

ing affection, encouragement, respect and all the exciting and gloomy things I have shared with them. I express my deepest gratitude to my parents, brothers, sisters, my wife, and my son for their emotional and moral support throughout my academic career and also for their tolerance, inspiration, and prayers.

Shahid Raza
Stockholm, May, 2013

This work has been performed in the Networked Embedded Systems (NES) Group that is a part of the Computer Systems Laboratory in the SICS Swedish ICT. This work is mainly financed by the Higher Education Commission (HEC) Pakistan in the form of PhD scholarship, and SICS Center for Networked Systems (CNS). The SICS CNS is funded by VINNOVA, SSF, KKS, ABB, Ericsson, Saab SDS, TeliaSonera, T2Data, Vendolocus, and Peerialism. This work has been partially supported by SSF, Uppsala VINN Excellence Center for Wireless Sensor Networks (WISENET), and European Commission with contract FP7-2007-2-224053 (CONET), FP7-2007-2-224282 (GINSENG), and FP7-ICT-2011.1.3- 288879 (CALIPSO).
The SICS Swedish ICT is sponsored by TeliaSonera, Ericsson, Saab SDS, FMV (Defence Materiel Administration), Green Cargo (Swedish freight railway operator), ABB, and Bombardier Transportation.

List of publications

Publications included in the thesis

1. Shahid Raza, Adriaan Slabbert, Thiemo Voigt, Krister Landernäs. Security Considerations for the WirelessHART Protocol. *In proceedings of 14th IEEE International Conference on Emerging Technologies and Factory Automation* (ETFA'09), September 22-26, 2009, Mallorca, Spain.

2. Shahid Raza, Simon Duquennoy, Tony Chung, Dogan Yazar, Thiemo Voigt, Utz Roedig. Securing Communication in 6LoWPAN with Compressed IPsec. *In proceedings 7th IEEE International Conference on Distributed Computing in Sensor Systems* (DCOSS '11), June 27-29 2011, Barcelona, Spain.

3. Shahid Raza, Simon Duquennoy, Joel Hoglund, Utz Roedig, Thiemo Voigt. Secure Communication for the Internet of Things - A Comparison of Link-Layer Security and IPsec for 6LoWPAN. *Journal of Security and Communication Networks*, Early View (), Wiley, 2012.

4. Shahid Raza, Hossein Shafagh, Kasun Hewage, René Hummen, Thiemo Voigt. Lithe: Lightweight Secure CoAP for the Internet of Things. [In Submission]

5. Shahid Raza, Linus Wallgren, Thiemo Voigt. SVELTE: Real-time Intrusion Detection in the Internet of Things. *Ad Hoc Networks* Journal, Elsevier, 2013. [Accepted]

6. Ibrahim Ethem Bagci, Shahid Raza, Tony Chung, Utz Roedig, Thiemo Voigt. Combined Secure Storage and Communication for the Internet of Things. *In proceedings of 10th IEEE International Conference on Sensing, Communication, and Networking* (SECON'13), June 24-27, 2013, New Orleans, USA.

Other publications
In addition to the papers included in the thesis I have also co-authored the following papers:

1. René Hummen, Jan H. Ziegeldorf, Hossein Shafagh, Shahid Raza, Klaus Wehrle. Towards Viable Certificate-based Authentication for the Web of Things. In proceedings of *ACM Workshop on Hot Topics on Wireless Network Security and Privacy*, co-located with ACM WiSec 2013, April 17-19, 2013, Budapest, Hungary.

2. Daniele Trabalza, Shahid Raza, Thiemo Voigt. INDIGO: Secure CoAP for Smartphones- Enabling E2E Secure Communication in the 6IoT. In proceedings of *International Conference on Wireless Sensor Networks for Developing Countries* (WSN4DC 13), April 24-26 2013, Jamshoro, Pakistan.

3. Ibrahim E. Bagci, Mohammad R. Pourmirza, Shahid Raza, Utz Roedig, Thiemo Voigt. Codo: Confidential Data Storage for Wireless Sensor Networks. In proceedings of *8th IEEE International Workshop on Wireless and Sensor Networks Security* (WSN'S 2012), in conjunction with 9th IEEE MASS'2012, October 8-12 2012, Las Vegas, Nevada, USA.

4. Shahid Raza, Daniele Trabalza, Thiemo Voigt. Poster Abstract: 6LoWPAN Compressed DTLS for CoAP. In proceedings of *8th IEEE International Conference on Distributed Computing in Sensor Systems* (DCOSS '12), 16-18 May 2012, Hangzhou, China.

5. Shahid Raza, Thiemo Voigt, Vilhelm Juvik. Lightweight IKEv2: A Key Management Solution for both Compressed IPsec and IEEE 802.15.4 Security. In *IETF Workshop on Smart Objects Security*, March 23, 2012, Paris, France.

6. Shahid Raza, Simon Duquennoy, Tony Chung, Dogan Yazar, Thiemo Voigt, Utz Roedig. Demo Abstract: Securing Communication in 6LoWPAN with Compressed IPsec. In proceedings *7th IEEE International*

Conference on Distributed Computing in Sensor Systems (DCOSS '11), 27-29 June 2011, Barcelona, Spain.

7. Shahid Raza, Gianluca Dini, Thiemo Voigt, and Mikael Gidlund. Secure Key Renewal in WirelessHART. In *Real-time Wireless for Industrial Applications* (RealWin'11), CPS Week, 11-16 April 2011, Chicago, Illinois, USA.

8. Shahid Raza, Thiemo Voigt, and Utz Roedig. 6LoWPAN Extension for IPsec. In *Interconnecting Smart Objects with the Internet Workshop*, 25 March 2011, Prague, Czech Republic.

9. Auriba Raza and Iftikhar A, Raja and Elisabet Lindgren and Shahid Raza. Land-use Change Analysis of District Abbottabad Pakistan: Taking Advantage of GIS and Remote Sensing. In proceedings of *4th International conference on Environmentally Sustainable Development*, June 2011, Pakistan.

10. Shahid Raza and Thiemo Voigt. Interconnecting WirelessHART and Legacy HART Networks. In proceedings of *1st International Workshop on Interconnecting Wireless Sensor Network* in conjunction with DCOSS'10., 21-23 June 2010, UC Santa Barbara, USA.

11. Shahid Raza, Thiemo Voigt, Adriaan Slabbert, Krister Landernäs. Design and Implementation of a Security Manager for WirelessHART Networks. In proceedings of *5th IEEE International Workshop on Wireless and Sensor Networks Security* (WSN'S 2009), in conjunction with MASS'2009, 12-15 Oct 2009, Macau SAR, P.R.C..

12. Joakim Eriksson, Fredrik Österlind, Thiemo Voigt, Niclas Finne, Shahid Raza, Nicolas Tsiftes, and Adam Dunkels. Demo abstract: accurate power profiling of sensornets with the COOJA/MSPSim simulator. In proceedings of *6th IEEE International Conference on Mobile Ad-hoc and Sensor Systems* (IEEE MASS 2009), 12-15 Oct 2009, Macau SAR, P.R.C..

Contents

I

Thesis

Chapter 1

Introduction

The Internet of Things (IoT) is a network of globally identifiable physical objects (or things), their integration with the Internet, and their representation in the virtual or digital world. In order to build the IoT, a wide range of technologies are involved. For example, RFID for location and device identification, improved personal and wide area networking protocols, web technologies, etc. These technologies help to build a virtual world of things on top of the physical world where things through Machine-to-Machine (M2M) communication talk to each other, through humans-to-machine interactions provide information to humans or take actions on human inputs, or act as passive entities to provide data to intelligent entities. Wireless Sensor Networks (WSN) is one such technology that connects the virtual world and the physical world where nodes can autonomously communicate among each other and with intelligent systems. This thesis focuses on the IoT formed through the interconnection of IP-connected WSNs and the Internet.

A conventional WSN is a network of sensor devices that sense and collect environmental data and cooperatively forward it to the sink node for further processing. These first generation WSNs lack any standardization support, are mostly used for environmental monitoring, and are deployed in remote areas such as forests, deserts, volcanos, and battlefields. Current WSNs are deployed in environments more close to humans and aimed for applications such as building automation, bridge and tunnel monitoring, industrial automation and control, and human sensing. The sink in current WSNs, such as WirelessHART networks, can query data from sensor nodes and/or send control messages to them. Though some standards are being developed for industrial WSNs such

as WirelessHART and ISA100.11a, there exists no specific standards for routing, addressing, security, etc. for such networks. Therefore, building current WSNs requires specialized skills in software and hardware development and protocol design. Also, conventional WSNs are not interoperable, require complex gateways, and are not scalable.

Sensor nodes are resource-constrained devices with limited storage and processing capabilities, are battery powered, and are connected through lossy links. The Internet Protocol (IP) is also proposed for WSN [1]; until recently IP has been assumed to be too heavyweight protocol to be used in WSN, as additional 40 bytes of IPv6 header are added in each packet [2]. However, IP offers interoperability, scalability, easy of programing, has ready to use hardware, eliminates the need of complex gateways, and has pool of readily available experts. Considering these advantages, IPv6 over low-powered Personal Area Network (6LoWPAN) [3, 4] is standardized. With the advent of 6LoWPAN, it is possible to use IP in resource-constrained WSNs in an efficient way [5]; such networks are called 6LoWPAN networks.

1.1 The IPv6-connected Internet of Things

With the introduction of 6LoWPAN compressed IPv6 in WSNs, resource constrained devices can be connected to the Internet. This hybrid network of the Internet and the IPv6 connected constrained devices form the IoT. Unlike the Internet where devices are mostly powerful and unlike typical WSN where devices are mostly resource constrained, the things in the IoT are extremely heterogeneous. An IoT device can be a typical sensor node, a light bulb, a microwave oven, an electricity meter, an automobile part, a smartphone, a PC or a laptop, a powerful server machine or even a cloud. Hence the number of potential devices that can be connected to the IoT are in hundreds of billions. This requires the use of IPv6 [16], a new version of the Internet Protocol that increases the address size from 32 bits to 128 bits (2^{128} unique addresses). Also, a number of protocols are being standardized to fulfill the specific needs of the IoT.

This section highlights the novel IoT technologies; Section 1.2 specifies the security requirements for the IoT that is developed based on these technologies; and Chapter 2 highlights challenges in providing secure communication in the IoT, and summarizes the contribution of this thesis towards securing the IoT.

6LoWPAN 6LoWPAN integrates IP-based infrastructures and WSNs by specifying how IPv6 packets are to be routed in constrained networks such as IEEE 802.15.4 networks [6]. To achieve this, the 6LoWPAN standard proposes context aware header compression mechanisms: the IP Header Compression (IPHC) for the IPv6 header, and Next Header Compression (NHC) for the IPv6 extension headers and the User Datagram Protocol (UDP) header. Due to the limited payload size of the link layer in 6LoWPAN networks, the 6LoWPAN standard also defines fragmentation and reassembly of datagram. 6LoWPAN defines a fragmentation scheme in which every fragment contains a reassembly tag and an offset. When security is enabled or for big application data size, the IEEE 802.15.4 frame size may exceed the Maximum Transmission Unit (MTU) size of 127 bytes; in that case additional fragment(s) are needed.

In order to allow compression of header like structures in the UDP payload and the layers above, an extension to the 6LoWPAN header compression, called Generic Header Compression (GHC) is also defined [7]. 6LoWPAN networks are connected to the Internet through the 6LoWPAN Border Router (6BR) that is analogous to a sink in a WSN. The 6BR preforms compression/decompression and fragmentation/assembly of IPv6 datagrams.

CoAP Due to the low-powered and lossy nature of wireless networks in the IoT, connection-less UDP, instead of stream-oriented TCP, is mostly used in the IoT. The synchronous Hyper Text Transfer Protocol (HTTP) is designed for TCP and is infeasible to use in the UDP-based IoT. Therefore, the Constrained Application Protocol (CoAP) [8], a subset of HTTP is being standardized as a web protocol for the IoT. CoAP is tailored for constrained devices and for machine-to-machine communication.

RPL Routing in constrained networks in the IoT, with limited energy and channel capacity, is achieved using the recently standardized the IPv6 Routing Protocol for Low-power and Lossy Networks (RPL) [9]. The RPL protocol creates a Destination-Oriented Directed Acyclic Graph (DODAG) that aims to prune path cost to the DAG root. RPL supports both uni-directional traffic to a DODAG root (typically the 6BR) and bi-directional traffic between constrained nodes and a DODAG root. Each node in the DODAG has a node ID (an IPv6 address), one or more parents (except for the DODAG root), and a list of neighbors. Nodes have a rank that determines their location relative to the neighbors and with respect to the DODAG root. The rank should always increase from the DODAG root towards nodes. In-network routing tables are maintained to

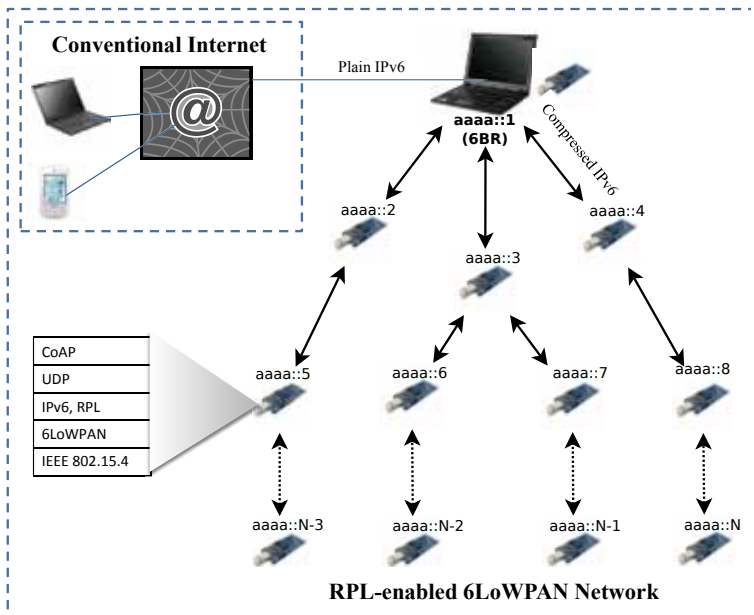

Figure 1.1: An interconnection of the Internet and WSNs using the novel IoT technologies 6LoWPAN, CoAP, and RPL which provide IPv6 support, web capabilities, and routing, respectively.

separate packets heading upwards and packets heading downwards in the network; this is called *storing* mode. RPL also supports *non-storing* mode where intermediate nodes do not store any routes.

Figure 1.1 shows an IoT setup that is build upon the novel technologies discussed in this section; the focus of this thesis is to protect this IoT with standard-based solutions.

1.2 Secure Internet of Things

IPv6 offers interconnection of almost every physical object with the Internet. This leads to tremendous possibilities to develop new applications for the IoT, such as home automation and home security management, smart energy moni-

toring and management, item and shipment tracking, surveillance and military, smart cities, health monitoring, logistics monitoring and management. Due to the global connectivity and sensitivity of applications, security in real deployments in the IoT is a requirement [10, 11]. The following security services [12] are necessary in the IoT.

Confidentiality: Messages that flow between a source and a destination could be easily intercepted by an attacker and secret contents are revealed. Therefor, these messages should be hidden from the intermediate entities; in other words, End-to-End (E2E) message secrecy is required in the IoT. Also, the stored data inside an IoT device should be hidden from unauthorized entities. *Confidentiality* services ensure this through encryption/decryption.

Data Integrity: No intermediary between a source and a destination should be able to undetectably change secret contents of messages, for example a medical data of a patient. Also, stored data should not be undetectably modified. Message Integrity Codes (MIC) are mostly used to provide this service.

Source Integrity or Authentication: Communicating end points should be able to verify the identities of each other to ensure that they are communicating with the entities who they claim to be. Different authentication schemes exist [13].

Availability: For smooth working of the IoT and access to data whenever needed, it is also important that services that applications offer should be always available and work properly. In other words, intrusions and malicious activities should be detected. Intrusion Detection Systems (IDSs) and firewalls, in addition to the security mechanisms above, are used to ensure availability security services.

Replay Protection: Last but not least, a compromised intermediate node can store a data packet and replay it at later stage. The replayed packet can contain a typical sensor reading (e.g. a temperature reading) or a paid service request. It is therefore important that there should be mechanisms to detect duplicate or replayed messages. Replay protection or freshness security services provide this, which can be achieved through integrity-protected timestamps, sequence numbers, nonces, etc.

In order to provide multi-faceted security, we need to ensure E2E communication security in the IoT, network security in 6LoWPAN networks, and also data-at-rest security to protect stored secrets and data.

1.2.1 Communication Security

Communication in the IoT should be protected by providing the security services discussed above. Using standardized Internet security mechanisms we

can provide communication security at different layers of the IP stack; each solution has its own pros and cons. Broadly speaking, the communication security can be provided E2E between source and destination, or on a per-hop basis between two neighboring devices. Table 1.1 shows an IoT stack with standardized security solution at different layers.

Link Layer: IEEE 802.15.4 Security

6LoWPAN networks use the IEEE 802.15.4 protocol [6] as link layer. 802.15.4 link-layer security [14] is the current state- of-the-art security solution for the IoT. The link layer security protects a communication on a per-hop base where every node in the communication path has to be trusted. A single pre-shared key is used to protect all communication. In case an attacker compromises one device it gains access to the key, and the security of the whole network is compromised. Per-hop security can detect the message modification on each hop unlike E2E where modified packets traverse the entire path up to the destination to be detected. Per-hop security with at least integrity protection should be used in 6LoWPAN networks to prevent unauthorized access through the radio medium, and to defend against effortless attacks launched to waste constrained resources. Though link-layer security is limited to securing the communication link between two neighboring devices, it is a flexible option and it can operate with multiple protocols at the layers above. For example with link-layer security enabled we can run both IP and non-IP protocols at the network layer.

Network Layer: IP Security

In the Internet and hence in the IoT, security at the network layer is provided by the IP Security (IPsec) protocol suite [15, 16, 17]. IPsec in transport mode provides end-to-end security with authentication and replay protection services in addition to confidentiality and integrity. By operating at the network layer, IPsec can be used with any transport layer protocol including TCP, UDP, HTTP, and CoAP. IPsec ensures the confidentiality and integrity of the IP payload using the Encapsulated Security Payload (ESP) protocol [17], and integrity of the IP header plus payload using the Authentication Header (AH) protocol [16]. IPsec is mandatory in the IPv6 protocol [2, 18] meaning that all IPv6 ready devices by default have IPsec support, which may be enabled at any time. Being a network layer solution, IPsec security services are shared among all applications running on a particular machine. However, being mandatory in IPv6, IPsec is one of the most suitable options for E2E security in the IoT, as mostly

IoT Layer	IoT Protocol	Security Protocol
Application	CoAP	User-defined
Transport	UDP	DTLS
Network	IPv6, RPL	IPsec, RPL security
6LoWPAN	6LoWPAN	None
Data-link	IEEE 802.15.4	802.15.4 security

Table 1.1: IoT stack with standardized security solutions.

only one application runs on a constrained device and the default security policies are enough for such scenarios. Furthermore, application developers require comparatively little effort to enable IPsec on IPv6 hosts, as it is already implemented at the network layer by device vendors.

Transport Layer: CoAP Security

Although IPsec can be used in the IoT it is not primarily designed for web protocols such as HTTP or CoAP. For web protocols Transport Layer Security (TLS) or its predecessor Secure Sockets Layer (SSL) is the most common security solution. The connection-oriented TLS protocol can only be used over stream-oriented TCP that is not the preferred method of communication for smart objects; due to lossy nature of low-power wireless networks it is hard to maintain a continuous connection in 6LoWPAN networks. An adaptation of TLS for UDP called Datagram TLS (DTLS) [19] is available. DTLS guarantees E2E security of different applications on one machine by operating between the transport and application layers. DTLS in addition to TLS that provides authentication, confidentiality, integrity, and replay protection, also provides protection against Denial of Service (DoS) attacks with the use of cookies. Though DTLS provides application level E2E security, it can only be used over the UDP protocol; TLS is used over TCP. The secure web protocol for the IoT, Secure CoAP (CoAPs), mandates the use of DTLS as the underlaying security solution for CoAP. Therefore, it is necessary to enable DTLS support in the IoT.

1.2.2 Network Security

Even with the communication security that protects the messages with confidentiality and integrity services, a number of attacks are possible against networks mainly to breach availability security services. These attacks are aimed to disrupt networks by interrupting, for example, the routing topology or by launching DoS attacks. Intrusion Detection Systems (IDS) are required to detect impostors and malicious activities in the network, and firewalls are necessary to block unauthorized access to networks. In the IoT, 6LoWPAN networks are vulnerable to a number of attacks from the Internet and from inside the network. Also, 6LoWPAN networks can become source of attacks against Internet hosts, as it is relatively easier to compromise a resource-constrained wireless node than a typical Internet host.

RPL [9], a routing protocol for low-power and lossy networks such as 6LoWPAN networks, is also prone to a number of routing attacks aimed to disrupt the topology. The IoT with 6LoWPAN networks running RPL, as shown in Figure 1.1, forms a network setup different from the typical WSNs. In the IoT, a 6BR is assumed to be always accessible, end-to-end message security is a requirement, and sensor nodes are identified by a unique IP address. In typical WSN there is no centralized manager and controller, security is usually ignored, and nodes are identifiable only within a WSN. Considering the novel characteristics of the IoT it is worth investigating the applicability of current IDS and firewall techniques in the IoT, or designing a novel IDS and firewall exploiting the contemporary IoT features and protocols.

1.2.3 Data Security

It is important to not only protect communication and networks but to also safeguard the stored sensitive data in an IoT device. Most of the IoT devices are tiny wirelessly connected resource-constrained nodes, and practically it is neither possible to physically guard each device nor to protect them with hardware-based tamper-resistant technologies such as with the use of smart cards or Trusted Platform Modules (TPM) [20]. Various software-based solutions exist that can be used to cryptographically secure stored data on nodes. For example, Codo [21] is a secure storage solution designed for the Contiki's Coffee File System [22]. There is also a need to design novel secure storage mechanisms in the context of IoT.

1.3 Research Methodology

The research methodology used in this thesis is mainly based on experimental research though analytical research is also adopted in the beginning of the thesis work. Experimental research that often starts with a concrete problem is used to evaluate the impact of one peculiar variable of a phenomenon by keeping the other variables controlled. Analytical research mainly deals with the testing of a concept that is not yet verified and specifying and inferring relationships by examining the concepts and information already available. We apply the analytical research methodology to perform a threat analysis of the WirelessHART network. We use the already known WirelessHART concepts and facts about security threats in the wireless medium and examine how the provided security mechanisms in WirelessHART guard against these threats.

Analyzing WirelessHART, a complex WSN standard, instilled me with a deep understanding of security mechanisms in low-power wireless networks and with typical limitations and issues in these networks. Based on the acquired knowledge, we develop lightweight communication, network, and data security solutions for the IoT where we mainly adapt an experimental research methodology as we have a concrete problem to solve. In order to build a communication security solution we first develop hypotheses or ideas about the architecture of IPsec, DTLS, and IEEE 802.15.4 security. We then formulate a design based on our hypothesis. To validate our hypothesis we implement and evaluate the proposed security solutions. We later examine the impact of our designed and implemented mechanisms on the IoT where we perform the evaluation of these mechanisms in a controlled experimental setup.

Realizing the need for the multi-faceted security in the IoT this thesis also provides network and data security where we develop a lightweight IDS and a novel combined secure storage and communication for the IoT. The research method we adapt here is experimental too. The first step towards solving this problem is to formulate a hypothesis, i.e., whether a novel IDS is needed for the IoT and what are the implications of a new storage model. The next step is to develop an architecture of the IDS and a secure storage mechanism that suits the IoT. To this end we provides detection techniques in the RPL-based 6LoWPAN networks and the new secure storage model. To validate our hypothesis and proposed algorithms we implement the IDS and the secure storage solution and perform extensive experiments. In the next step we analyze our experimental results that show that the proposed IDS suites the IoT and detects routing attacks in the RPL-based 6LoWPAN networks, and the new secure storage solution is more efficient than the conventional secure storage mechanisms.

1.4 Thesis Outline

This dissertation has two parts. The first part is the introduction of the thesis and second part is a collection of six papers.

Chapter 2 describes the scientific contributions of this thesis and summaries the results. Chapter 3 highlights the research contributions of this thesis and references the corresponding publications. Chapter 4 discusses the related work that motivates the need for new security solutions for the IoT. Chapter 5 concludes the thesis and provides future work; this ends the first part of the thesis.

Chapter 2

Challenges and Contributions

On one hand, constrained environments in the IoT have attributes similar to WSNs such as limited energy, processing, and storage resources, lossy wireless links, unguarded deployments, and multi-hop communication. On the other hand, the IoT is expected to have IPv6, UDP, and web support. Providing security is challenging in the Internet and in typical WSNs. It is even more challenging to enable security services in the IoT. This is because the devices are extremely heterogeneous, mostly deployed in unattended environments but closer to humans than typical WSN nodes, are globally accessible, mostly connected through lossy wireless links, require multi-hop communication, and use recent IoT protocols such as 6LoWPAN, CoAP, and RPL. This thesis provides multi-faceted security solutions for the IoT. The main contributions of this thesis are:

- It provides lightweight solutions based on standardized protocols to securely connect IoT devices. This enables the devices in the constrained environments to securely communicate with typical Internet hosts using lightweight yet standard compliant Internet security protocols such as IPsec and DTLS.
- It also contributes towards protecting 6LoWPAN networks against intrusion attempts and unauthorized access.
- In addition to communication and network security, this thesis also pro-

vides solutions to protect stored data inside a resource-constrained IoT node.

The previous chapter has highlighted security services and the standard-based security solutions in the IoT. This chapter highlights the challenges in providing security in the IoT and summarizes the contributions of this thesis.

2.1 Secure Communication: Message Security

The IoT is a hybrid network of Internet and constrained networks. Communication in the IoT can be secured with *(i)* lightweight security protocols proposed for constrained environments such as WSNs, *(ii)* novel security protocols that meet the specific requirements of the IoT, or *(iii)* established security protocols already used in the Internet. Security protocols proposed for WSNs are not designed for IP networks. Therefore, their use in the IoT requires modification of these protocols and corresponding provisioning in the current Internet. Designing novel security protocols for the IoT may result in more efficient and lightweight solutions; however, these protocols too require changes in the Internet. As the current Internet is huge, consisting of billions of devices, any security solution that requires modifications or provisions in the current Internet is not practical. It is however worth investigating the applicability of established Internet security technologies in the IoT. The primary challenge that may hinder the use of these security solutions in the IoT is that the Internet protocols are not designed for resource constrained devices but for standard computers where energy sources, processing capability, and storage space are not main constraints. One of the contributions in this thesis is to adapt the communication security protocols standardized for the Internet in the IoT, by making them lightweight yet standard compliant.

It is important that the messages in the IoT are E2E protected with confidentiality and integrity services. Also, at least integrity protection should be employed on a per-hop base in the wirelessly connected 6LoWPAN networks. Towards this end, this thesis presents the first compressed yet standard compliant IPsec for the E2E security between IoT hosts and compressed DTLS for E2E security between applications in the IoT. In order to protect messages on a per-hop base between two neighboring devices, implementation and evaluation of link layer security solutions are also provided.

***Lightweight IPsec*:** This thesis presents the first lightweight design, implementation, and evaluation of IPsec for resource-constrained devices. With 6LoW-

PAN header compression, the IPsec AH header size is reduced from 24 bytes to 16 bytes, and the ESP header size is reduced from 18 bytes to 14 bytes. This results in a lower number of bits being transmitted, more space for application data, and may avoid 6LoWPAN fragmentation; ultimately, the energy consumption is reduced as the energy consumed by radio on transmission and reception is much higher than used by microprocessor on local processing. Paper C also shows that with hardware aided crypto processing the energy overhead is further reduced by 50%. For example, when carrying 512 bytes over 4 hops, pure software-based IPsec AH involves an overhead of 26%, which is reduced to 11% with the help of hardware AES. Contrary to the common belief that IPsec is too heavy for constrained devices [3, 23], IPsec is faster than the IEEE 802.15.4 security as the number of hops grows or the data size increases. This is because the compression mechanisms substantially reduce the data overhead on fragmented traffic, and cryptographic operations are only performed at the end hosts and not at each hop as in the case of 802.15.4 security.

***Lightweight DTLS*:** Though IPsec is a feasible solution for the IoT, it is less suitable for web-based applications in the IoT. CoAP is being standardized as a web protocol for the IoT, which mandates the use of DTLS as an underlaying security solution to enable secure CoAP (CoAPs). To provide standard based E2E security in the CoAPs-enabled IoT applications, this thesis presents the first lightweight DTLS and hence CoAPs. Like IPsec, DTLS is designed for the conventional Internet and not for the resource-constrained IoT, as it is a chatty protocol and requires numerous message exchanges to establish a secure session. The DTLS header compression is based on 6LoWPAN NHC [4]. Employing these compression mechanisms significantly reduces the DTLS header sizes and ultimately results in fast and energy efficient communication compared with plain DTLS. For example, by employing the proposed mechanisms the DTLS Record header size is reduced by 62% while still maintaining the E2E standard compliance between two communication end points. The quantitative evaluation in Paper D shows that the energy overhead is significantly reduced especially when the 6LoWPAN fragmentation is employed. The use of compressed DTLS makes CoAPs considerably lightweight and a feasible security protocol for the IoT.

Realizing that smartphones with sensing capabilities, human interaction, Internet connectivity, and relatively powerful processing and storage capacities, will be an integral part of the IoT, we also provide standard-based design, implementation, and evaluation CoAPs for Android powered smartphones [24]. This paper is not included in the core contributions of this thesis.

***IEEE 802.15.4 Security*:** Prior to our work on IPsec and DTLS, 802.15.4 security was the only standard-based security solution available in 6LoWPAN networks. The IEEE 802.15.4 standard provides the link layer security to protect communication between two neighboring nodes. Link layer security is not a replacement of network or transport layer security. For 6LoWPAN networks with multiple hops, Paper C recommends that at least integrity protection should be enabled at the link layer to grand access in the wireless medium and to detect the effortless data modification attacks as early as possible. However, there is a tradeoff between the overhead of providing security at the link layer and the overhead of routing faked packets through multiple hops to the destination where they are ultimately detected. Therefore, when E2E security is provided at the network or upper layers, enabling or disabling link layer security should be carefully decided; the goal is to minimize resource usage.

In order to enable link layer security, this thesis provides an implementation of IEEE 802.15.4 security for the Contiki OS and evaluates it in a 6LoWPAN network. For 6LoWPAN networks with less hops and small data size, 802.15.4 link layer security is efficient when compared with the network layer security. Since it does not provide E2E security, the 802.15.4 security is not a replacement for IPsec or DTLS; it is therefore recommended that either IPsec or DTLS should be used in conjunction to the 802.15.4 security.

Figure 2.1 shows an IoT setup with the list of lightweight security solutions in the resource-constrained 6LoWPAN network and the corresponding plain technologies on the Internet side. The 6BR converts the compressed protocols in plain protocols and vice versa.

2.2 Secure Network: Intrusion Detection

Though communication security protects messages, networks are still vulnerable to a number of attacks aimed to disrupt the network. Intrusion Detection Systems (IDSs) and firewalls guard against such attacks. As the IoT shares characteristics with WSNs, the available IDSs for WSNs could be used in the IoT. However, most of these approaches assume that there is no centralized management and control point, no message security, and sensor nodes are uniquely identified only within WSNs. In the IoT, nodes are globally identifiable by an IP address, the 6BR is presumed to be always reachable to connect 6LoWPAN networks with the Internet, and E2E message security is a must. It is therefore worth designing a new IDS for the IoT by exploiting these novel characteristics. In spite of these characteristics, developing an IDS for the IoT

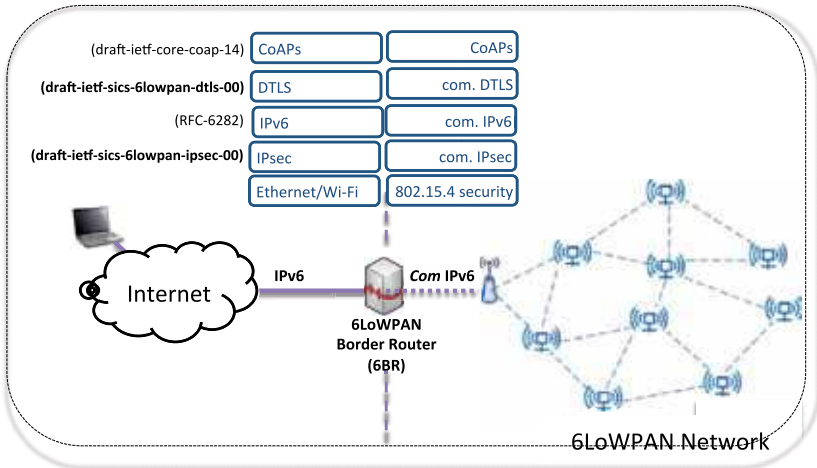

Figure 2.1: An IoT setup protected with proposed lightweight security solution, and a set of operations performed at the 6BR.

is challenging due to global accessibility, constrained resources, lossy links, and use of recent IoT protocols such as RPL.

In order to protect 6LoWPAN networks against intrusions and unwanted access this thesis provides an IDS and a mini-firewall. The IDS is designed for 6LoWPAN networks that use RPL as a routing protocol. Paper E develops a novel architecture based on a hybrid of centralized and distributed approaches. The detection algorithms in the IDS detect intrusions against RPL networks by employing contemporary lightweight detection techniques. A mini-firewall, also based on a hybrid approach, is also developed. The detection techniques are evaluated against sinkhole and selective forwarding attacks. The results show that the IDS can detect these attacks with a high true positive and detection rate. Also, the energy and ROM/RAM overhead of the IDS and the firewall are acceptable in 6LoWPAN networks.

2.3 Secure Device: Data Security

In a typical storage model, data is stored in an encrypted form along with its cryptographic hash [25], and when a remote host requests data, it is decrypted and its integrity is verified, re-encrypted and integrity protected with commu-

nication security mechanisms, and transmitted. This way the resource hungry cryptographic operations are performed twice.

With the recent advancement of flash memory, relatively more storage is now available in constrained devices. It is therefore worth exploiting the use of this additional memory in order to minimize energy consumption. Towards this end this thesis presents combined secure storage and communication mechanisms for the IoT. The proposed combined secure storage and communication mechanism, presented in Paper F, eliminates these double cryptographic operations. This work is build upon the IPv6, IPsec, and 6LoWPAN standards as a standard compliant system is more acceptable than a proprietary solution. In this new secure storage solution, data is stored on the flash file system such that it can be directly used for secure transmission. In the current design and implementation, data is protected with IPsec's ESP protocol and both the ESP header and encrypted data are stored on a flash. Prior to this operation, IP datagram header contents of future transmissions are considered in order to comply with the IPsec standard. The evaluation shows that an IP based combined secure storage and communication solution for the IoT is possible and that this can save up to 71% of a node's security related processing.

2.4 Security Analysis of WirelessHART

WirelessHART [26], though resource constrained, is a bidirectional network of relatively powerful devices and has a central network manager and controller. WirelessHART, currently the only WSN standard, designed primarily for industrial process automation and control, is well designed for other aspects than security. The provided security is spread throughout the WirelessHART specifications. The network designers and device vendors have ambiguities regarding the complete security architecture of the WirelessHART, the strength of the provided security, the security keys needed, and the functionalities and placement of Security Manager. This thesis discusses, in Paper A, the strengths and weaknesses of the provided security mechanisms in the form of a threat analysis where we analyze the WirelessHART security against the well-known threats in the wireless medium and propose recommendations to mitigate the impact of these threats. It also elaborates the functions of security manager and its placement in the network. In addition to security analysis of WirelessHART, we have also developed a WirelessHART security manager [27] and proposed secure integration of WirelessHART and legacy HART networks [28]. However, these papers are not included in the core contributions of this thesis.

The industrial community is also moving towards IP communication. This is apparent from the fact that the proposed industrial standard ISA 100.11a is IP based, and efforts are underway to apply IP communication in WirelessHART, formally named HART IP, and in ZigBee named ZigBee IP.

2.5 Standardization of Proposed Solutions

The contributions presented in this thesis mainly target HCF WirelessHART, and IETF 6LoWPAN, CoAP and RPL. During this thesis period, I attended meetings of both the HCF and IETF standardization bodies. This helped me to know the current status of the standardization efforts, to make people aware of our work, and ultimately the standardization of the work proposed in this thesis. I have attended the WirelessHART Working Group meetings in Florence and in Naples, the Internet Architecture Board (IAB) official workshop and tutorial along with the IETF 80th meeting in Prague, the IETF 83rd meeting in Paris and ETSI CoAP Plugtests. Currently, our IETF compressed IPsec draft is under review and we are working on IETF compressed DTLS draft. An ultimate aim is the inclusion of the solutions proposed in this thesis in the standard specifications. I have also published the IPsec work in the IAB workshop on Interconnecting Smart Objects with the Internet [29], and the proposed Internet Key Exchange (IKE) work in the IETF Workshop on Smart Objects Security [30].

Chapter 3

Summary of Papers

This thesis is a collection of six papers. Paper A studies the security threats in WirelessHART. Papers B-D investigate the communication security in the IoT. Paper E explores the network security in the IoT, and Paper F investigates the protection of stored data inside a node.

Paper A performs a threat analysis of WirelessHART and highlights the important security aspects of WirelessHART. Also, it stipulates the specifications of the WirelessHART security manager, its placement in the network and interactions with the other WirelessHART devices. Paper B, C, and D investigate lightweight communication security in the IoT with standard-based solutions: IPsec, DTLS, and IEEE 802.15.4. Paper E studies the protection of the IoT against network and routing attacks, and presents an IDS and firewall for RPL-based 6LoWPAN networks. Paper F explores the security of stored data inside a resource-constrained node. It presents a novel combined secure storage and communication solution for the IoT, with the special focus on minimizing cryptographic operations.

Paper A, B, and F are published in renowned international peer-reviewed conferences, Paper C and E are published in ISI indexed referenced journals, and Paper D is under submission to a journal.

3.1 Security Considerations for the WirelessHART Protocol

Shahid Raza, Adriaan Slabbert, Thiemo Voigt, Krister Landernäs. Security Considerations for the WirelessHART Protocol. *In Proceedings of 14th IEEE International Conference on Emerging Technologies and Factory Automation* (ETFA'09), September 22-26, 2009, Mallorca, Spain.

Summary

WirelessHART is a secure and reliable communication standard for industrial process automation. The WirelessHART specifications are well organized in all aspects except security: there are no separate specifications of security requirements or features. Rather, security mechanisms are described throughout the documentation. This impedes implementation of the standard and development of applications since it requires close knowledge of all the core specifications on the part of the developer.

We have thoroughly discussed the security features in the WirelessHART standard and analyzed the specified security features against the available threats in the wireless medium. We have also identified some security limitations in the standard. However, the provided security in the wireless medium, although subjected to some threats due to its wireless nature, is strong enough to be used in industrial process control environments. The physical protection of the WirelessHART devices is very important to avoid device cloning and stealing security secrets, which will lead to other security attacks. Also, the careful implementation of the Network Manager is very important. The WirelessHART standard does not enforce security in the core/wired network but the connections between the wired devices must be secured. The standard provides core security services including confidentiality, integrity, authentication, and availability; however, other security services such as non-repudiation, authorization or access control, and accounting are yet to be provided.

Contribution

In this paper we provide a comprehensive overview of WirelessHART security where we analyze the provided security mechanisms against well-known threats in the wireless medium, and propose recommendations to mitigate shortcomings. Furthermore, we elucidate the specifications of the Security Manager, its placement in the network, and interaction with the Network Manager.

My Contribution

I reviewed the WirelessHART security, performed the threat analysis of WirelessHART, and wrote the first draft of the paper.

3.2 Securing Communication in 6LoWPAN with Compressed IPsec

Shahid Raza, Simon Duquennoy, Tony Chung, Dogan Yazar, Thiemo Voigt, Utz Roedig. Securing Communication in 6LoWPAN with Compressed IPsec. *In Proceedings 7th IEEE International Conference on Distributed Computing in Sensor Systems* (DCOSS '11), June 27-29 2011, Barcelona, Spain.

Summary

Real-world deployments of wireless sensor networks (WSNs) require secure communication. It is important that a receiver is able to verify that sensor data was generated by trusted nodes. It may also be necessary to encrypt sensor data in transit. WSNs will be an integral part of the Internet and IPv6 and 6LoWPAN are the protocol standards that are expected to be used in this context. IPsec is the standard method to secure Internet communication and we investigate if IPsec can be extended to sensor networks. Towards this end, we have presented the first IPsec specification and implementation for 6LoWPAN. We have extensively evaluated our implementation and demonstrated that it is possible and feasible to use compressed IPsec to secure communication between sensor nodes and hosts in the Internet.

Contribution

In this paper we provide End-to-End (E2E) secure communication between IP enabled sensor networks and the traditional Internet. We present the first compressed lightweight design, implementation, and evaluation of 6LoWPAN extension for IPsec. We give a specification of IPsec for 6LoWPAN including definitions for AH and ESP extension headers. Prior to this work no specification for IPsec in the context of 6LoWPAN existed. We present the first implementation of IPsec for 6LoWPAN networks. We show that it is practical and feasible to secure WSN communication using IPsec. We evaluate the performance of our IPsec 6LoWPAN implementation in terms of code size, packet

overheads and communication performance. Our results show that the overhead comparable to the overhead of generally employed 802.15.4 link-layer security while offering the benefit of true E2E security.

My Contribution

I am the main author of the paper. I proposed the 6LoWPAN compression, contributed in implementation, and designed and performed most of the evaluation. I wrote most of the paper.

3.3 Secure Communication for the Internet of Things A Comparison of Link-Layer Security and IPsec for 6LoWPAN

Shahid Raza, Simon Duquennoy, Joel Höglund, Utz Roedig, Thiemo Voigt. Secure Communication for the Internet of Things - A Comparison of Link-Layer Security and IPsec for 6LoWPAN. *Journal of Security and Communication Networks*, DOI: 10.1002/sec.406, Early View (January 12, 2012), Wiley, 2012.

Summary

The future Internet of Things will be an all-IP network. As it will be the foundation of many services, our daily life will depend on its availability and reliable operation. It is therefore important to find mechanisms providing security in the IoT. As the existing IEEE 802.15.4 link-layer security does not provide the required end-to-end security, alternative or complementary mechanisms must be found. In this paper we have shown that IPsec implemented through 6LoWPAN extensions is a feasible option for providing end-to-end security in the IoT, and IEEE 802.15.4 security, at least integrity protection, is also needed. This paper presents a thorough evaluation of the proposed IPsec solution and compares its performance with IEEE 802.15.4 link-layer security.

Contribution

In Paper B we present a 6LoWPAN/IPsec solution and perform a preliminary performance analysis of the overall system. In this paper we extend our pre-

vious work (Paper B) in several aspects. First, we describe in this paper Encapsulating Security Payload (ESP) for 6LoWPAN/IPsec while our previous work only discussed in detail the Authentication Header (AH). Second, we compare the 6LoWPAN/IPsec solution with the commonly employed 802.15.4 link-layer security, where we also implement IEEE 802.15.4 security for the Contiki OS. Third, we present a thorough testbed performance evaluation of the 6LoWPAN/IPsec solution and 802.15.4 security. We experimentally show that 6LoWPAN/IPsec outperforms 802.15.4 link-layer security as the payload size and/or the number of hops increases.

My Contribution

I designed the 6LoWPAN extension for IPsec's ESP. I implemented IEEE 802.15.4 security for the Contiki OS, and I performed most of the evaluation. I wrote the first draft of the paper.

3.4 Lithe: Lightweight Secure CoAP for the Internet of Things

Shahid Raza, Hossein Shafagh, Kasun Hewage, René Hummen, Thiemo Voigt. Lithe: Lightweight Secure CoAP for the Internet of Things. [In Submission]

Summary

CoAP enabled hosts will be an integral part of the Internet of Things (IoT). Furthermore, real world deployments of CoAP supported devices require security solutions. To this end, DTLS is the standard protocol to enable secure CoAP (CoAPs). In this paper, we investigate if the overhead of DTLS can be reduced by 6LoWPAN header compression, and present the first DTLS header compression specification for 6LoWPAN. We quantitatively show that DTLS can be compressed and its overhead can be significantly reduced using the 6LoWPAN standardized mechanisms. Our implementation and evaluation of compressed DTLS demonstrate that it is possible to reduce the CoAPs overhead, as the DTLS compression is efficient in terms of energy consumption and network- wide response time, when compared with plain CoAPs. The difference between compressed DTLS and plain DTLS is very significant, if the use of plain DTLS results in 6LoWPAN fragmentation.

Contribution

In this paper, we present Lithe- an integration of DTLS and CoAP for the IoT. With Lithe, we additionally propose a novel DTLS header compression scheme that aims to significantly reduce the header overhead of DTLS leveraging the 6LoWPAN standard. Most importantly, our proposed DTLS header compression scheme does not compromise the end-to-end security properties provided by DTLS. At the same time, it considerably reduces the number of transmitted bytes while maintaining DTLS standard compliance. The main contributions of this paper are: *(i)* we provide novel and standard compliant DTLS compression mechanisms that aim to increase the applicability of DTLS and, thus, CoAPs for constrained devices, and *(ii)* we implement the compressed DTLS in an OS for the IoT and evaluate it on real hardware; the results quantitatively show that Lithe is more efficient in many aspects than the plain CoAP/DTLS.

My Contribution

I am the main author of the paper. I proposed the compressed DTLS, and contributed in the implementation and evaluation of the compressed DTLS. I wrote most of the paper.

3.5 SVELTE: Real-time Intrusion Detection in the Internet of Things

Shahid Raza, Linus Wallgren, Thiemo Voigt. SVELTE: Real-time Intrusion Detection in the Internet of Things. *Ad Hoc Networks* Journal, Elsevier, 2013 [Accepted].

Summary

In the Internet of Things (IoT), resource-constrained things are connected to the unreliable and untrusted Internet via IPv6 and 6LoWPAN networks. Even when they are secured with encryption and authentication, these things are exposed both to wireless attacks from inside the 6LoWPAN network and from the Internet. Since these attacks may succeed, Intrusion Detection Systems (IDS) are necessary. Currently, there are no IDSs that meet the requirements of the IPv6-connected IoT since the available approaches are either customized for Wireless Sensor Networks (WSN) or for the conventional Internet. To this

end we present SVELTE, the first IDS for the IoT. We implement and evaluate SVELTE and show that it is indeed feasible to use it in the context of RPL, 6LoWPAN, and the IoT. To guard against global attacks we also design and implement a mini- firewall.

Contribution

In this paper we design, implement, and evaluate a novel intrusion detection system for the IoT that we call SVELTE. In our implementation and evaluation we primarily target routing attacks such as spoofed or altered information, sinkhole, and selective-forwarding. However, our approach can be extended to detect other attacks. We implement SVELTE in the Contiki OS and thoroughly evaluate it. Our evaluation shows that in the simulated scenarios, SVELTE detects all malicious nodes that launch our implemented sinkhole and/or selective forwarding attacks. However, the true positive rate is not 100%, i.e., we have some false alarms during the detection of malicious nodes. Also, SVELTE's overhead is small enough to deploy it on constrained nodes with limited energy and memory capacity.

My Contribution

I proposed the IDS for the IoT. I contributed in the development of the intrusion detection infrastructure, detection algorithms, and the 6Mapper. I designed the evaluation and I wrote the first draft of the paper.

3.6 Combined Secure Storage and Communication for the Internet of Things

Ibrahim Ethem Bagci, Shahid Raza, Tony Chung, Utz Roedig, Thiemo Voigt. Combined Secure Storage and Communication for the Internet of Things. *In proceedings of 10th IEEE International Conference on Sensing, Communication, and Networking* (SECON'13), June 24-27, 2013, New Orleans, USA.

Summary

The future Internet of Things (IoT) may be based on the existing and established Internet Protocol (IP). Many IoT application scenarios will handle sensitive data. However, as security requirements for storage and communication

are addressed separately, work such as key management or cryptographic processing is duplicated. Our proposed secure storage and communication framework is based on the established IPv6/6LoWPAN protocols. IPv6/6LoWPAN defines IPsec/ESP (Encapsulating Security Payload) that provides encryption and authentication of transmitted data packets. We use the same cryptographic methods and data formats defined by ESP for data processing before storage. This requires us to store not only data but also all header information that is involved in the cryptographic processing. We have shown that this is possible within the context of the IP protocol family. The described solution requires additional storage space on nodes. However, we believe that currently available flash memory sizes can absorb these overheads. Data on nodes must be secured when stored and transported in order to implement a comprehensive security solution. As resource-constrained embedded systems are limited in resources it is necessary to find efficient solutions. The proposed framework combining security aspects of storage and communication can help to achieve this goal.

Contribution

In this paper we present a framework that allows us to combine secure storage and secure communication in the IP-based IoT. We show how data can be stored securely such that it can be delivered securely upon request without further cryptographic processing. The main contributions of this paper are: *(i)* the definition of a framework for combined secure storage and communication for IP/6LoWPAN networks, *(ii)* an implementation of the framework for the Contiki operating system, and *(iii)* a detailed evaluation of the performance gains of the framework. Our prototype implementation shows that combined secure storage and communication can reduce security related real-time processing on nodes dramatically (up to 71% reduction). As shown, this can be achieved while decreasing as well a nodes power consumption (up to 32.1%).

My Contribution

I contributed in the idea of this paper, provided the initial IPsec support, and participated in writing and reviewing the paper.

Chapter 4

Related Work

There is unanimous consensus among the IoT research community that security is an important requirement in the IoT [10, 11, 31, 32, 33]. A number of security protocols has been proposed for resource-constrained WSNs [12]. However, these security protocols are often tailored to the specific application requirements and do not consider interoperability with Internet protocols. On the other hand, the IoT security protocols require interoperability with Internet protocols.

Though Garcia-Morchon et al. [31] provide general security needs in the IoT and highlight the importance of standard-based security protocols, they do not propose any adaptations in Internet protocols which make them feasible to use in the IoT. Also, no quantitative evaluation shows the applicability of standard Internet security protocols in the IoT. Granjal [32] accentuates the need for E2E security in the IoT, and shows with empirical evaluation the limitations of current sensing platforms. The community of IoT security researchers has analyzed security challenges in the IP-based IoT [33] and solutions that improve or modify standard IP security protocols that meet the requirements of resource-constrained devices. They conclude that security architectures should fit device capabilities, that proposed security protocols should ensure scalability, that cross layer interactions such as for key management is important in multi-layered solutions, and that standardization of these security solutions is important for interoperability.

4.1 Communication Security

Communication security based on End-to-End (E2E) message protection and authentication is well-recognized in the research community [10, 11, 32, 34]. Yu et al. [10] propose E2E secure communication between WSNs and Internet. They use asymmetric cryptography for key management and authentication and delegate resource hungry operations to a gateway. This leads to a need for a complex gateway, which also breaks pure E2E security between sensor nodes and hosts on Internet.

Cryptographic processing is one of the main resource hungry tasks while providing communication security. These operations include encryption and decryption, key and hash generation, and sign and verify hashes. Wander et al. [35] compare two most well-know asymmetric algorithms, RSA and Elliptic Curve Cryptography (ECC) [36], on sensor nodes and conclude that ECC is more efficient than RSA, and asymmetric cryptography is viable for constrained hardware. Later, in order to make ECC viable for WSNs, a lot of research work has focused on reducing complexity of asymmetric cryptographic algorithms, ultimately improving efficiency of key distribution protocols. For example, TinyECC [37] and NanoECC [38] use ECC in order to make cryptography feasible on resource-constrained devices. Wood et al. [39] and Hu et al. [40] have demonstrated efficient cryptography for smart objects using dedicated crypto hardware support. We have also shown that use of crypto hardware significantly reduces the overhead of cryptographic operations (Paper C). Liu et al. [41] and Chung et al. [42] describe key distribution mechanisms that save scarce bandwidth in resource constrained networks. These improvements make cryptographic mechanisms in the context of WSNs more viable but an important issue remains: a standardized way of implementing security services is missing and for each deployment unique customized solutions are created. This thesis provides lightweight solutions based on standardized protocols to securely connect IoT devices.

4.1.1 IEEE 802.15.4 Security

IEEE 802.15.4 security provides standardized mechanisms for message authentication and encryption on a per-hop base in 6LoWPAN networks. However, these mechanisms are difficult to implement on resource constrained sensor nodes, as cryptographic mechanisms can be expensive in terms of code size and processing speed. Furthermore, messages leaving the 802.15.4 network and continuing to travel on an IP network are not protected by link-layer secu-

rity mechanisms. Therefore, in many solutions, a separate security mechanism is added to protect data traveling between Internet hosts and border routers. One such example is the ArchRock PhyNET [43] that applies IPsec in tunnel mode between the border router and Internet hosts. HIP DEX [44] is another solution that can be used directly as a keying mechanism for a MAC layer security protocol. Wood et al. [39] also propose a solution to secure link-layer communication in TinyOS for IEEE 802.15.4-based WSN. Recently, Roman et al. proposed key management systems for sensor network in the context of the IoT [45] that are applicable to link-layer security. We also implement standardized 802.15.4 security for 6LoWPAN networks with hardware-aided crypto operations and show that it is viable to use 802.15.4 security in constrained environments (Paper C); however, 802.15.4 security only protects communication between two neighboring devices.

4.1.2 Transport Layer

End-to-end security can be provided by using Transport Layer Security (TLS) [46], or by its old version SSL. TLS/SSL has been proposed as a security mechanism for the IoT by Hong et al. [47]. Their evaluation shows that this security mechanism is indeed quite costly in terms of time and energy during full SSL handshake and a data packet transfer. Foulagar et al. propose a TLS implementation for smart objects [48]. However, this solution involves the border router to reduce cryptographic computational effort on smart objects and cannot be considered a full E2E solution. Brachmann et al. [49] propose TLS-DTLS mapping to protect the IoT. However, their solution requires the presence of a trusted 6BR that break E2E security at the 6BR. Kothmayr et al. [50] investigate the use of DTLS in 6LoWPANs with a Trusted Platform Module (TPM) to get hardware support for the RSA algorithm. However, in addition to specialized hardware requirement, they have used DTLS as it is without using any compression method which would shorten the lifetime of the entire network due to the redundancy in transmitted data.

Granjal et al. [34] evaluate the use of DTLS as it is with CoAP for secure communication. They note that payload space scarcity would be problematic with applications that require larger payloads. As an alternative, they suggest to employ security at other networking layers such as compressed form of IPsec. Brachmann et al. [51] provide an overview of state-of-the-art security solutions for a CoAP-based applications, and discuss the feasibility of DTSL, TLS, IPsec, or combination of these for E2E security and secure multicast communication. They assume pre-shared keys in their proposals due to

resource-constrained nature of the nodes. Recently, Koeh et al. in an IETF draft discuss the implications of securing the IP-connected IoT with DTLS [52] and propose an architecture for secure network access and management of unicast and multicast keys with extended DTLS. Garcia et al. [11] also propose and compare pre-shared based Host Identity Protocol (HIP) and DTLS as key management, secure network access, and secure communication protocols. They conclude that though HIP is efficient, it is not widely available in the current Internet; on the other hand DTLS in its current form is heavy for constrained devices and requires optimizations.

The above solutions either review the use of (D)TLS in the IoT or propose architectures that break E2E security. We reduce the overhead of DTLS in CoAP-based IoT by employing 6LoWPAN header compression mechanisms, and implement and evaluate it in an IoT setup on real hardware (Paper D). Our solution is DTLS standard complaint and ensures E2E security between CoAP applications. However, we rely on pre-shared key for initial authentication during handshake. In another work [53], we propose design ideas to reduce the overhead of the two-way certificate-based DTLS handshake. We suggest (i) pre-validation of certificates at the trusted 6BR, (ii) session resumption to avoid the overhead of a full handshake, and (iii) handshake delegation to the owner of the resource-constrained device. This work in making certificate-based authentication viable for the IoT is complementary to our work on compressed DTLS (Paper D).

Researchers are also investigating vulnerabilities in the DTLS protocol. Nadhem et al. recently demonstrated successful attacks against the DTLS protocol [54, 55].

4.1.3 IPsec

IPsec ensures the confidentiality and integrity of transport-layer headers and integrity of IP headers, which cannot be done with higher-level solutions as TLS. For these reasons, the research community [56, 57, 58] and 6LoWPAN and CoRE standardization groups [4, 59] consider IPsec a potential security solution for the IoT. On the other hand, some have regarded IPsec heavy for constrained environments [60].

We propose a standard-compliant IPsec extension for 6LoWPAN (Paper B) and evaluate it on real hardware in an IoT setup. Granjal et al. investigate the use of IPsec for 6LoWPAN [61]. However, they do not provide exact specifications of the required 6LoWPAN headers. Furthermore, no implementation is provided and no detailed evaluation of possible communication performance

is given. In their study they analyze the execution times and memory requirements of cryptographic algorithms they propose for 6LoWPAN/IPsec integration. We design, implement, and evaluate 6LoWPAN compressed IPsec for the IoT, and quantitatively compare it with the 802.15.4 security (Paper C). We propose to use IPsec in transport mode that enables E2E security between the communicating endpoints. We implement our compressed IPsec in the Contiki OS [62]. Recently, Jorge et al. [63] have extended our 6LoWPAN compressed IPsec (Paper C) and included support for IPsec in tunnel mode. They have implemented and evaluated their proposal in TinyOS.

4.1.4 Key Management in the IoT

Key Management Systems (KMSs) proposed for WSNs are tailored for specific scenario [12] and are not interoperable with Internet protocols. The KMS for the IoT should be based on standard protocols. The standard-complaint security protocol DTLS has inherited automatic KMS that the Handshake protocol provides. For key management in the resource-constrained WSNs and 6LoWPANs, pre-shared keying is still the state-of-art mechanism. Recent IETF proposal on the use of DTLS in the IoT also relies on pre-shared keys [52]. For scalable and automatic key management we have shown the viability of certificate-based DTLS in the context of IoT [53].

IPsec relies on Internet Key Exchange (IKE) [64] for key management. Kivinen proposes a lightweight IKEv2 [65] that includes the minimal set of features and does not include the optional features. This proposal too relies on shared secret for authentication and considers certificate-based authentication too heavy for the IoT. Roman et al. propose key management systems for the IoT [45] that are applicable to link-layer security. The IEEE 804.15.4 protocol does not provide a KMS. We have proposed an adaptation of the IKE that extends its key management capabilities to the IEEE 802.15.4 protocol [30]. Recently, Jennings has proposed a transitive trust provisioning for constrained devices [66], which uses a one-time password to enroll a constrained device in an IoT.

4.2 Network Security

A number of attacks against the IoT have been identified [67] in addition to those against WSN [68] that are also applicable to the IoT. Therefore, it is important to have systems that detect such attacks. The concept of intrusion detec-

tion is quite old and extensive research is carried out in this field mostly against the Internet attacks and attacks against WSN. However, no IDS are specifically designed in the context of IoT. Most of the IDS approaches for WSN are based on a distributed architecture and are built on the assumption that there is no centralized management and control point. A common IDS approach for WSNs is to utilize several special nodes distributed evenly throughout the network. These special nodes can either be physically different [69] or dynamically distributed throughout the network [70, 71]. In real deployments, however, it cannot be guaranteed that particular nodes are always present in specific locations in the network; also, the cost of employing mobile agents that move through the network might be too high. Clustering based approaches have similar issues as each cluster often requires a powerful entity for coordination [72]. The IoT has a novel architecture where the 6BR is always assumed to be accessible and is a potential place for centralized management and control.

Many IDS approaches are based upon watchdog techniques [70, 73] which could be used in the IoT. In addition to being distributed and fully deployed on sensor nodes, a general problem with watchdog-based approaches is that they require promiscuous listening, which consumes a lot of power and therefore is not suitable for constrained devices. Advanced anomaly detection approaches are proposed [74, 75], not primarily for WSNs, which on one hand can detect many intrusions efficiently but on the other hand requires intelligent learning, which is both expensive and difficult in low-power 6LoWPAN networks. Most current IDS approaches require different routing schemes that are not based on standardized mechanisms. As far as we are aware, no approach is built around 6LoWPAN and RPL in the context of the IoT. Our solution is the first design, implementation, and evaluation of the IDS for the IoT (Paper E).

4.3 Secure Storage

Solutions for secure communication and secure storage of data in the IP based IoT exist, but these functions are generally designed and operated independent of each other. There are a number of secure storage solutions available [21, 76, 77, 78]. Codo [21] is a security extension for the Coffee filesystem [22] in the Contiki OS. Codo optimizes performance of security operations by enabling caching of data for bulk encryption and decryption. We use Codo as a base and present combined secure storage and communication for the IoT, which is faster and more energy efficient than the conventional separate secure storage and communication solutions.

Chapter 5

Conclusions and Future Work

5.1 Conclusions

The IoT is becoming a reality and serious standardization efforts are underway to interconnect the IoT devices using the IP protocols such as CoAP, 6LoWPAN, RPL, etc. IP networks will be the foundation of many services and our daily life will depend on their availability. Security is must in the IoT. Due to the sensitivity of potential applications, not just protection of communication, but a multi-faceted security is important. This thesis has presented lightweight yet standard compliant security solutions to protect communication, constrained networks, as well as stored data in devices in the IoT.

Towards secure communication in the IoT, this thesis has investigated the use of IPsec, DTLS, and the IEEE 802.15.4 security. For web-based applications in the IoT, DTLS is well suited for E2E security, and the optimized DTLS presented in this thesis has lower overhead in terms of energy consumption and response time than the plain DTLS. With currently available hardware capabilities in the IoT devices, pre-shared key authentication during the DTLS handshake is still an acceptable solution, as proposed by other recent works on DTLS as well. IPsec, mandated by IPv6, is a security solution to protect communication at the network layer, which provides security between two machines. This thesis shows that it is viable to provide E2E security in the IoT with 6LoWPAN compressed IPsec in transport mode. The evaluation

of compressed IPsec in transport mode shows that the ROM/RAM, energy, and response time overhead is acceptable. It is also shown that, contrary to the common believe, IPsec is more efficient than IEEE 802.15.4 security in 6LoWPAN networks with multiple hops and for larger message sizes. The IEEE 802.15.4 security at the link layer and upper layer security solutions (e.g. IPsec and DTLS) are not replacements for reach other. For the early identification of certain attacks (such as a data modification attack) and hence for the efficient use of network resources, in addition to E2E security solutions, link-layer security is also important in multi-hop 6LoWPAN networks.

For multi-faceted security, it is important that the IoT is protected against internal and external intrusions. Towards this end, this thesis has proposed and developed a lightweight IDS for 6LoWPAN networks that use RPL as routing protocol in the IoT. To guard against global attacks we have also designed and implemented a mini-firewall. The detection algorithms in the proposed IDS currently target spoofed or altered information, sinkhole and selective forwarding attacks. However, our IDS infrastructure is extensible and more attack detection mechanisms can be added.

Most of the IoT devices are tiny wireless devices and it is relatively easier to capture and clone them. Therefore, this thesis has also proposed a secure storage solution in the context of IoT. Unlike typical secure storage mechanisms that require separate cryptographic operations for storage and for communication security, this thesis has presented a combined secure storage and communication. Though this solution requires a little more storage space, it can reduce security related real-time processing on nodes up to 71%, and power consumption is reduced up to 32.1% when data is stored in ESP protected format.

5.2 Future Work

Pre-shared keying is still the state-of-art key management solution in the IoT. IPsec mandates pre-shared key, and CoAPs that relies on DTLS also proposes the use of pre-shared key in addition to RawPublicKey and certificate-based authentication. The communication security solutions presented in this thesis rely on shared secret key. However, with the advancement of hardware, more storage and processing capabilities with efficient energy usage are expected in the IoT devices. With these increased capabilities it may be wise to deploy certificate-based cryptography in the IoT. We have already proposed optimizations in the certificate-based authentication during the DTLS hand-

shake to make DTLS a viable solution for automatic key management, secure network access, and session negotiation. Currently, we are working on the implementation of these proposals, and plan to evaluate the full certificate-based DTLS on real hardware. Also, we plan to investigate the use of certificate-based IKEv2 for automatic key management for IPsec. In order to make IKEv2 fit for constrained environments, we have already proposed preliminary adaptations in the IKEv2. We plan to implement and evaluate the enhance IKEv2 protocol that, in addition to IPsec, also provides key management solution for the 802.15.4 security.

In the current work, we have evaluated the proposed solutions in testbeds. We plan to deploy these security technologies in real IoT deployments and evaluate them together. In parallel, we are also working on enhancements in our IDS and firewall for the IoT and extending it with more detection capabilities.

This thesis focuses on the security aspects of the IoT. Another important concern in the IoT is privacy. The importance of privacy is well-studied in the context of IoT [79, 80, 81]. However, the current work on privacy in the IoT focuses on vision, requirements, and challenges, and lacks the quantitative analysis of enabling privacy. We plan to investigate the adaptation of Privacy Enhancing Techniques (PETs) [82, 83] in the context of the IoT with empirical analysis, and plan to quantify the overhead of providing privacy in constrained environments. Some of other open security issues and challenges in the IoT are:

- Use of asymmetric cryptography with certificate-based mutual authentication in the IoT.
- Secure bootstrapping of things in the IoT with ease-of-use.
- Security and privacy of sensor data inside a cloud environment, in an integrated system of a cloud and the IoT [84, 85].
- Secure management of IoT domains.

Bibliography

[1] Adam Dunkels. Full tcp/ip for 8-bit architectures. In *Proceedings of the 1st international conference on Mobile systems, applications and services*, pages 85–98. ACM, 2003.

[2] S. Deering and R. Hinden. Internet Protocol, Version 6 (IPv6) Specification. RFC 1883 (Proposed Standard), December 1995. Obsoleted by RFC 2460.

[3] N. Kushalnagar, G. Montenegro, and C. Schumacher. IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals. RFC 4919, August 2007. http://www.ietf.org/rfc/rfc4919.txt.

[4] J. Hui and P. Thubert. Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks. RFC 6282, September 2011. http://www.ietf.org/rfc/rfc6282.txt.

[5] Jonathan W Hui and David E Culler. Ip is dead, long live ip for wireless sensor networks. In *Proceedings of the 6th ACM conference on Embedded network sensor systems*, pages 15–28. ACM, 2008.

[6] IEEE Computer Society. Ieee std. 802.15.4-2006, 2006.

[7] C. Bormann. 6LoWPAN Generic Compression of Headers and Header-like Payloads, September 2012. http://tools.ietf.org/html/draft-bormann-6lowpan-ghc-05.

[8] Z. Shelby, K. Hartke, and C. Bormann. Constrained Application Protocol (CoAP), March 2013. http://tools.ietf.org/html/draft-ietf-core-coap-14.

[9] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, and R. Alexander. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. RFC 6550, March 2012. http://www.ietf.org/rfc/rfc6550.txt.

[10] Hong Yu, Jingsha He, Ting Zhang, Peng Xiao, and Yuqiang Zhang. Enabling end-to-end secure communication between wireless sensor networks and the internet. *World Wide Web*, pages 1–26, 2012.

[11] Oscar Garcia-Morchon, Sye Loong Keoh, Sandeep Kumar, Pedro Moreno-Sanchez, Francisco Vidal-Meca, and Jan Henrik Ziegeldorf. Securing the ip-based internet of things with hip and dtls. In *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks*, pages 119–124. ACM, 2013.

[12] Javier López and Jianying Zhou. *Wireless Sensor Network Security*. IOS Press, 2008.

[13] Richard E Smith. *Authentication: from passwords to public keys*. Addison-Wesley Longman Publishing Co., Inc., 2001.

[14] Naveen Sastry and David Wagner. Security considerations for ieee 802.15. 4 networks. In *Proceedings of the 3rd ACM workshop on Wireless security*, pages 32–42. ACM, 2004.

[15] S. Kent and R. Atkinson. Security architecture for the internet protocol, 1998. http://www.ietf.org/rfc/rfc2401.txt.

[16] S. Kent. IP Authentication Header. RFC 4302, 2005. http://tools.ietf.org/html/rfc4302.

[17] S. Kent. IP Encapsulating Security Payload. RFC 4303, 2005. http://tools.ietf.org/html/rfc4303.

[18] R. Atkinson. Security Architecture for the Internet Protocol. RFC 1825 (Proposed Standard), August 1995. Obsoleted by RFC 2401.

[19] E. Rescorla and N. Modadugu. Datagram Transport Layer Security Version 1.2. RFC 6347, January 2012. http://www.ietf.org/rfc/rfc6347.txt.

[20] Trusted Platform Module (TPM) Work Group. TCG specification architecture overview (TPM 2007), 2007. http://www.trustedcomputinggroup.org/.

[21] Ibrahim Ethem Bagci, Mohammad Reza Pourmirza, Shahid Raza, Utz Roedig, and Thiemo Voigt. Codo: Confidential data storage for wireless sensor networks. In *8th IEEE International Workshop on Wireless and Sensor Networks Security (WSNS 2012)*, Las Vegas, Nevada, USA, October 2012.

[22] Nicolas Tsiftes, Adam Dunkels, He Zhitao, and Thiemo Voigt. Enabling large-scale storage in sensor networks with the coffee file system. In *Proceedings of the 2009 International Conference on Information Processing in Sensor Networks*, pages 349–360, Washington, DC, USA, 2009. IEEE Computer Society.

[23] Andrey Khurri, Dmitriy Kuptsov, and Andrei Gurtov. On application of host identity protocol in wireless sensor networks. In *Mobile Adhoc and Sensor Systems (MASS), 2010 IEEE 7th International Conference on*, pages 358–345. IEEE, 2010.

[24] Thiemo Voigt Daniele Trabalza, Shahid Raza. Indigo: Secure coap for smartphones- enabling e2e secure communication in the 6iot. In *International Conference on Wireless Sensor Networks for Developing Countries (WSN4DC'13)*, pages 0–12, Jamshoro, Pakistan, April 2013.

[25] Bart Preneel. Cryptographic hash functions. *European Transactions on Telecommunications*, 5(4):431–448, 1994.

[26] Anna N. Kim, Fredrik Hekland, Stig Petersen, and Paula Doyle. When hart goes wireless: Understanding and implementing the wirelesshart standard. *IEEE International Conference on Emerging Technologies and Factory Automation*, pages 899–907, September 2008.

[27] Shahid Raza, Thiemo Voigt, Adriaan Slabbert, and Krister Landernas. Design and implementation of a security manager for wirelesshart networks. In *Proceedings of the IEEE 6th International Conference on Mobile Adhoc and Sensor Systems (IEEE MASS 2009)*, pages 995–1004, Macau, China, 2009.

[28] Shahid Raza and Thiemo Voigt. Interconnecting wirelesshart and legacy hart networks. In *Proceedings of the 6th IEEE International Conference on Distributed Computing in Sensor Systems Workshops (IEEE DCOSSW 2010)*, Santa Barbara, USA, 2010.

[29] Shahid Raza, Thiemo Voigt, and Utz Roedig. 6lowpan extension for ipsec. *Proceedings of the IETF-IAB International Workshop on Interconnecting Smart Objects with the Internet*, 2011.

[30] Shahid Raza, Thiemo Voigt, and Vilhelm Juvik. Lightweight ikev2: A key management solution for both compressed ipsec and ieee 802.15.4 security. *Proceedings of the IETF International Workshop on Smart Object Security*, March 2012.

[31] O. Garcia-Morchon, S. Keoh, S. Kumar, R. Hummen, , and R. Struik. Security Considerations in the IP-based Internet of Things, March 2013. http://tools.ietf.org/html/draft-garcia-core-security-05.

[32] Jorge Granjal, Edmundo Monteiro, and Jorge Sa Silva. On the effectiveness of end-to-end security for internet-integrated sensing applications. In *Green Computing and Communications (GreenCom), 2012 IEEE International Conference on*, pages 87–93. IEEE, 2012.

[33] Tobias Heer, Oscar Garcia-Morchon, René Hummen, Sye Loong Keoh, Sandeep S Kumar, and Klaus Wehrle. Security challenges in the ip-based internet of things. *Wireless Personal Communications*, 61(3):527–542, 2011.

[34] Jorge Granjal, Edmundo Monteiro, and Jorge Sa Silva. On the feasibility of secure application-layer communications on the web of things. In *Local Computer Networks (LCN), 2012 IEEE 37th Conference on*, pages 228–231. IEEE, 2012.

[35] Arvinderpal S Wander, Nils Gura, Hans Eberle, Vipul Gupta, and Sheueling Chang Shantz. Energy analysis of public-key cryptography for wireless sensor networks. In *Pervasive Computing and Communications, 2005. PerCom 2005. Third IEEE International Conference on*, pages 324–328. IEEE, 2005.

[36] Victor S Miller. Use of elliptic curves in cryptography. In *Advances in CryptologyCRYPTO85 Proceedings*, pages 417–426. Springer, 1986.

[37] A. Liu and P. Ning. TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks. In *7th International Conference on Information Processing in Sensor Networks (IPSN'08)*, Washington, DC, USA, 2008.

[38] P. Szczechowiak, L. Oliveira, M. Scott, M. Collier, and R. Dahab. Nanoecc: Testing the limits of elliptic curve cryptography in sensor networks. In *5th European conference on Wireless Sensor Networks (EWSN'08)*, Bologna, Italy, 2008.

[39] A. Wood and J. Stankovic. Poster abstract: AMSecure - secure link-layer communication in TinyOS for IEEE 802.15.4-based wireless sensor networks. In *4th ACM Conference on Networked Embedded Sensor Systems (SenSys'06)*, Boulder, USA, 2006.

[40] W. Hu, P. Corke, W. Shih, and L. Overs. secfleck: A public key technology platform for wireless sensor networks. In *6th European conference on Wireless Sensor Networks (EWSN'09)*, Cork, Ireland, 2009.

[41] D. Liu and P. Ning. Establishing pairwise keys in distributed sensor networks. In *10th ACM conference on Computer and communications security (CCS)*, New York, NY, USA, 2003.

[42] A. Chung and U. Roedig. DHB-KEY: An Efficient Key Distribution Scheme for Wireless Sensor Networks. In *4th IEEE International Workshop on Wireless and Sensor Networks Security (WSNS'08)*, Atlanta, USA, 2008.

[43] ArchRock Corporation. Phynet n4x series, 2008.

[44] R. Moskowitz. HIP Diet EXchange (DEX), November 2012. http://tools.ietf.org/html/draft-moskowitz-hip-rg-dex-06.

[45] Rodrigo Roman, Cristina Alcaraz, Javier Lopez, and Nicolas Sklavos. Key management systems for sensor networks in the context of the internet of things. *Computers & Electrical Engineering*, 37(2):147–159, 2011.

[46] T. Dierks and E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246 (Proposed Standard), August 2008. http://www.ietf.org/rfc/rfc5246.txt.

[47] S. Hong, D. Kim, M. Ha, S. Bae, S. J. Park, W. Jung, and J. Kim. Snail: an ip-based wireless sensor network approach to the internet of things. *Wireless Communications, IEEE*, 17(6):34–42, 2010.

[48] S. Fouladgar, B. Mainaud, K. Masmoudi, and H. Afifi. Tiny 3-tls: A trust delegation protocol for wireless sensor networks. In *3rd European Workshop on Security and Privacy in Ad-Hoc and Sensor Networks (ESAS'03)*, Hamburg, Germany, 2006.

[49] M. Brachmann, S. L. Keoh, O. G. Morchon, and S. S. Kumar. End-to-end transport security in the IP-Based Internet of Things. In *Computer Communications and Networks (ICCCN), 2012 21st International Conference on*, pages 1 –5, August 2012.

[50] T. Kothmayr, C. Schmitt, W. Hu, M. Brunig, and G. Carle. A DTLS based end-to-end security architecture for the Internet of Things with two-way authentication. In *Local Computer Networks Workshops, 2012 IEEE 37th Conference on*, pages 956–963. IEEE, 2012.

[51] Martina Brachmann, Oscar Garcia-Morchon, and Michael Kirsche. Security for practical coap applications: Issues and solution approaches. *GI/ITG KuVS Fachgesprch Sensornetze (FGSN). Universitt Stuttgart*, 2011.

[52] S. Keoh, S. Kumar, and O. Garcia-Morchon. Securing the IP-based Internet of Things with DTLS, February 2013. http://tools.ietf.org/html/draft-keoh-lwig-dtls-iot-01.

[53] R. Hummen, J. H. Ziegeldorf, H. Shafagh, S. Raza, and K. Wehrle. Making Certificate-based Authentication Viable for the Web of Things. In *Proceedings of the 2nd ACM Workshop on Hot Topics on Wireless Network Security and Privacy (HotWiSec)*, April 2013.

[54] N.J. AlFardan and K.G. Paterson. Lucky thirteen: Breaking the TLS and DTLS record protocols. In *34th IEEE Symposium on Security and Privacy*, San Francisco, California, 2013.

[55] Nadhem J AlFardan and Kenneth G Paterson. Plaintext-recovery attacks against datagram tls. In *Network and Distributed System Security Symposium (NDSS 2012)*, 2012.

[56] J. Granjal, R. Silva, E. Monteiro, J. Sa Silva, and F. Boavida. Why is IPsec a viable option for wireless sensor networks . In *WSNS2008*, Atlanta, USA, September 2008.

[57] R. Riaz, Ki-Hyung Kim, and H.F. Ahmed. Security analysis survey and framework design for ip connected lowpans. In *ISADS '09*, mar. 2009.

[58] R. Roman and J. Lopez. Integrating wireless sensor networks and the internet: a security analysis. *Internet Research*, 19(2):246–259, 2009.

[59] C. Bormann. Using CoAP with IPsec, December 2012. http://tools.ietf.org/html/draft-bormann-core-ipsec-for-coap-00.

[60] C. Alcaraz, P. Najera, J. Lopez, and R. Roman. Wireless sensor networks and the internet of things: Do we need a complete integration? In *1st International Workshop on the Security of the Internet of Things (SecIoT'10)*, Tokyo, Japan, 2010.

[61] Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva. Enabling network-layer security on ipv6 wireless sensor networks. In *IEEE Global Communications Conference (GLOBECOM,10)*, Miami, USA, 2010.

[62] Adam Dunkels, Bjorn Gronvall, and Thiemo Voigt. Contiki - a lightweight and flexible operating system for tiny networked sensors. In *Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks*, pages 455–462. IEEE Computer Society, 2004.

[63] J. Granjal, E. Monteiro, and J. S. Silva. Network-layer security for the Internet of Things using TinyOS and BLIP. *International Journal of Communication Systems*, 2012.

[64] C. Kaufman, P. Hoffman, Y. Nir, and P. Eronen. Internet Key Exchange Protocol Version 2 (IKEv2). RFC 5996 (Proposed Standard), September 2010. http://www.ietf.org/rfc/rfc5996.txt.

[65] T. Kivinen. Minimal IKEv2, April 2013. http://tools.ietf.org/html/draft-kivinen-ipsecme-ikev2-minimal-01.

[66] C. Jennings. Transitive Trust Enrollment for Constrained Devices, April 2013. http://tools.ietf.org/html/draft-jennings-core-transitive-trust-enrollment-01.

[67] O. Garcia-Morchon, R. Hummen, S.S. Kumar, R. Struik, and S.L. Keoh. Security Considerations in the IP-based Internet of Things, March 2012. http://tools.ietf.org/html/draft-garcia-core-security-04.

[68] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad hoc networks*, 1(2):293–315, 2003.

[69] I.M. Atakli, H. Hu, Y. Chen, W.S. Ku, and Z. Su. Malicious node detection in wireless sensor networks using weighted trust evaluation. In *Proceedings of the 2008 Spring simulation multiconference*, pages 836–843. Society for Computer Simulation International, 2008.

[70] R. Roman, J. Zhou, and J. Lopez. Applying intrusion detection systems to wireless sensor networks. In *Proceedings of IEEE Consumer Communications and Networking Conference*, pages 640–644, 2006.

[71] T.H. Hai, E.N. Huh, and M. Jo. A lightweight intrusion detection framework for wireless sensor networks. *Wireless Communications and mobile computing*, 10(4):559–572, 2009.

[72] C. Rong, S. Eggen, and H. Cheng. An efficient intrusion detection scheme for wireless sensor networks. *Secure and Trust Computing, Data Management, and Applications*, 187:116–129, 2011.

[73] Sergio Marti, T. J. Giuli, Kevin Lai, and Mary Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, MobiCom '00, pages 255–265, New York, NY, USA, 2000. ACM.

[74] Amitabh Mishra, Ketan Nadkarni, and Animesh Patcha. Intrusion detection in wireless ad hoc networks. *Wireless Communications, IEEE*, 11(1):48–60, 2004.

[75] Kai Hwang, Min Cai, Ying Chen, and Min Qin. Hybrid intrusion detection with weighted signature generation over anomalous internet episodes. *Dependable and Secure Computing, IEEE Transactions on*, 4(1):41–55, 2007.

[76] Neerja Bhatnagar and Ethan L. Miller. Designing a secure reliable file system for sensor networks. In *Proceedings of the 2007 ACM workshop on Storage security and survivability*, pages 19–24, 2007.

[77] Joao Girao, Dirk Westhoff, Einar Mykletun, and Toshinori Araki. Tinypeds: Tiny persistent encrypted data storage in asynchronous wireless sensor networks. *Ad Hoc Netw.*, 5:1073–1089, September 2007.

[78] Wei Ren, Yi Ren, and Hui Zhang. Hybrids: A scheme for secure distributed data storage in wsns. In *Proceedings of the 2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing - Volume 02*, pages 318–323. IEEE Computer Society, 2008.

[79] Rolf H Weber. Internet of things–new security and privacy challenges. *Computer Law & Security Review*, 26(1):23–30, 2010.

[80] Vladimir Oleshchuk. Internet of things and privacy preserving technologies. In *Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology, 2009. Wireless VITAE 2009. 1st International Conference on*, pages 336–340. IEEE, 2009.

[81] Carlo Maria Medaglia and Alexandru Serbanati. An overview of privacy and security issues in the internet of things. In *The Internet of Things*, pages 389–395. Springer, 2010.

[82] Peter Langendörfer, Michael Maaser, Krzysztof Piotrowski, and Steffen Peter. Privacy enhancing techniques: A survey and classification. *Handbook of Research on Wireless Security*, 1, 2008.

[83] G De Moor, B Claerhout, and F De Meyer. Privacy enhancing techniques. *Meth Info Med*, 42:148–153, 2003.

[84] Simon Duquennoy et. al. SicsthSense. http://www.sense.sics.se.

[85] Cosm - connect to your world. https://cosm.com.