University of Zurich[UZH]

FACHARBEIT – Communication Systems Group, Prof. Dr. Burkhard Stiller

# Classification and Analysis of Security Protocols and Algorithms for Constrained Networks

*Niko Van Wyk*
*Zurich, Switzerland*
*Student ID: 06-921-308*

Supervisor: Dr. Corinna Schmitt, Bruno Rodrigues
Date of Submission: September 6, 2017

University of Zurich
Department of Informatics (IFI)
Binzmühlestrasse 14, CH-8050 Zürich, Switzerland

CSG
Department of Informatics
Communication Systems Group

Facharbeit
Communication Systems Group (CSG)
Department of Informatics (IFI)
University of Zurich
Binzmühlestrasse 14, CH-8050 Zürich, Switzerland
URL: http://www.csg.uzh.ch/

# Abstract

There is no doubt that the Internet of Things (IoT) is one of the largest future visions. The development and research progress grows exponentially just like the number of IoT devices and applications in use. As a core part of the IoT, Wireless Sensor Networks (WSN) are busy sensing environmental conditions, ranging from simple things such as temperature, location or heart rate, to complex things such as the water level in a coffee machine or video from public places. As networks, WSNs are, of course, also exposed to attacks, including known attacks of existing network technologies as well as new ones, which arose specifically from WSNs. In this context, security in WSNs is of major concern and security solutions have to be adapted by means of new attacks. This results in a large number of journal papers on a broad range of security-related issues. This Facharbeit (FA) analyzes the large number of security-related journal papers in the field of WSNs in the period from 2012 to 2017, and proposes the most comprehensive classification scheme according to which this bandwidth can be categorized in order to master the large mass. Subsequently, the classification scheme is exemplarily evaluated with an in-depth security analysis of selected security protocols and algorithms from journal papers with regard to well-known security fundamentals.

# Contents

# Chapter 1

# Introduction

The technological progress of the last decades allowed a miniaturization of processing equipped devices. Thus, these devices can move out of the context of a user desktop environment. But miniaturization may lead, among other limiting factors such as costs, also to devices that are constrained in computational capacity, power supply and memory. These constrained devices can form a network, which may lead in turn to a constrained network, as it may suffer from the devices' constraints. [1, 46]

One possible scope of application is the autonomous sensing and interaction of the physical environment for which Wireless Sensor Networks (WSN), sometimes also called Wireless Sensor and Actuator Network (WSAN), are designed. WSNs can be seen as a part of the emerging Internet of Things (IoT), which describes a future vision of ambient intelligence where objects of all kinds, the "things", are equipped with a processor and are uniquely identifiable in the Internet. The sensing devices used in WSNs are constrained in computational capacity, power supply, and memory depending on stakeholders' requests such as size, costs or applicability in a scenario. Thus, WSNs are constrained networks. [1, 46]

Moreover, the search for security-related journal papers in scientific research databases as part of this Facharbeit (FA) showed that the term "constrained network" is rarely used; rather the search resulted in papers concerned with security in WSNs to date, allowing this FA to equally and interchangeably use the terms "constrained network" and "WSN".

Popular applications of WSNs are disaster relief (e.g., wildfire detection), environmental monitoring and control, smart buildings, agriculture, military (e.g., battlefield surveillance), machine surveillance and preventive maintenance, medicine and health care, logistics, animal tracking, traffic management, and public safety. Logistics or animal tracking is mainly used with radio-frequency identification (RFID), which is also considered as a WSN since they "sense" the existence through identification. Moreover, passive RFID tags are very constrained, resulting in a constrained network. [1, 5, 6]

This FA deals with security in WSNs and proposes a classification scheme for security-related algorithms and protocols. Subsequently, the classification scheme is exemplarily evaluated with selected protocols and algorithms which are also analyzed for their security, particularly with regard to well-known security fundamentals.

The remainder of this FA is organized as follows: Chapter 2 gives some needed background about WSNs and their security issues in order to present in Chapter 3 a classification scheme of security-related protocols and algorithms for WSNs. Chapter 4 provides an instance of the proposed classification scheme. Selected protocols and algorithms between 2012 and 2017 are classified according to the proposed scheme and analyzed for their security. The results of the analysis are presented in a comparative table. Chapter 5 concludes this FA with a summary.

# Chapter 2

# Background

In this chapter, a brief introduction to WSNs and their related security issues is given to provide the needed background in order to present the classification scheme and provide a security analysis of selected security protocols and algorithms in the next chapters.

## 2.1 Wireless Sensor Networks

A Wireless Sensor Network (WSN) consists of small sensing devices, called nodes, deployed in an environmental area where a measure of a value or values is required. These can be variables such as temperature, loudness, vibration, pressure, pH, humidity, location, motion, light such as cameras, and many more. Nodes are equipped with a sensor (or actuator), power supply, processor, memory, and transceiver. The power supply is either a battery or might be an energy recovery module such as solar cells, but seldom wired power. Due to stakeholders' requests and application scenarios, there may be several limitations on the sensing devices and the network itself. These devices may be constrained in computational capacity, power supply and memory, resulting in a network that may also suffer from these limitations. Such networks may be constrained in, e.g., low bandwidth, high packet loss rate, or limited overall lifetime. However, not only the devices' constraints may lead to a constrained network. For example, harsh environmental conditions must also be considered depending on the area of operation. [1, 46]

Sensed data has to be transmitted from a constrained device (e.g., sensor node) to an end-point (e.g., called gateway, sink, base station or server) where it is further processed due to the limited resources of the device. This communication usually is done in a wireless manner. Due to the possible constraints of nodes resulting in low transmission ranges of nodes and a possible spacious field of sensing, the transmission of data is done in a hop-by-hop fashion towards the sink. Thus, nodes have not only to sense and transmit data but also must forward data and route data packets. The sink is then connected via classic network schemes (e.g., TCP/IP-based Internet or Ethernet) with an end-point that can be an end-user or a data center for instance, but is not considered as a part of WSNs. [1, 7]

The architecture of WSNs is usually either flat or hierarchical. In a flat WSN, all nodes are similarly important to the network, i.e., they offer the same functionalities and are logical not distinguishable. In a hierarchy-based WSN, nodes have different tasks and may also differ in physical characteristics (e.g., fixed power supply or higher computational capacity) to build up a logical clustered network structure. So-called cluster heads, which may be physically the same nodes as ordinary sensor nodes or resource richer nodes, form a cluster in which the sensor nodes in its group are connected to, either directly or by multi-hop via other ordinary sensor nodes in the same cluster. The cluster heads are then interconnected to each other and finally to a sink. A data packet from an ordinary sensor node is then always first transmitted to the cluster head where it may be intermediately processed (e.g., data aggregation) and then sent to a sink. It is also possible to introduce additional intermediate hierarchical levels of devices in order to make the hierarchy even finer. [1, 23, 29, 35, 36]

Since WSNs are all about the sensed data and the delivery to a sink, the data are more important than the source which delivered the data; that is, WSNs are data-centric networks. This is in high contrast to classic networks like the TCP/IP-based Internet in which the focus lies on the transfer of data between two specific entities, each equipped with a network address. Such networks are thus address-centric. [1]

Due to the possible heavy constraints of sensor nodes, all programming should be focused on these constraints to save resources. In this context, the term data aggregation is also of major importance, which is mostly applied in hierarchical architectures and takes place at intermediate hierarchical levels such as cluster heads. Suppose several nodes detect the same event and send the notification to their cluster head, which then should transmit it to a sink. As WSNs are data-centric, one is only interested that an event occurred. Thus, the cluster head can aggregate all the same event notifications from all nodes reporting and send this smaller data packet to a sink instead of forwarding all reported data packets in order to save its resources. [1, 23]

Another key concern for networks is security. Nodes and the WSN may be heavily constrained, which overall makes classic, well-known and established security approaches as used in wired networks with resource rich entities not applicable for constrained networks [5, 8]. In the next sections, security aspects are dealt with in more detail.

## 2.2 Security aspects

The constraints mentioned in Section 2.1 make a WSN very different from classic networks such as the TCP/IP-based Internet or WLAN as the following summary shows [5, 6, 7]:

- There may be no absolutely central node depending on use cases and communication standards
- Depending on application scenario, nodes must be able to be self-organizing due to the lack of infrastructure

- A WSN may consist of thousands of nodes depending on use cases and communication standards
- The network topology may be very volatile and unpredictable due to possible node failures or node mobility
- Besides sensing, nodes are also responsible for data forwarding and routing in a hop-by-hop manner towards a sink
- Nodes may be prone to failures due to harsh environments and energy constraints depending on use cases and stakeholders' requests
- Nodes may be constrained in computational capacity, power supply and memory
- WSNs are data-centric networks

These major differences—especially those due to the constraints—require the development and use of special security protocols and algorithms to match the particular requirements of a WSN. Often, the broad range of real-world WSN-based applications even leads to the development of scenario-specific security protocols, schemes or frameworks, such as surveillance of coal mines [37], smart vehicular systems [38], e-health applications [39, 40], or underwater acoustic networks [41]. Nevertheless, WSNs are networks, and security in networks is designed according to well-known security goals or security fundamentals requested by stakeholders. Selected important security fundamentals are described in the following.

**Confidentiality** becomes important in case of transmitting sensitive data (e.g., IP address, phone number, location, bank account). It defines a set of rules that limits the data access to authorized entities or persons [48]. Thus, attackers cannot gain information such as secret keys or knowledge such as traffic analysis [2, 8, 9]. Confidentiality is seen as the most important security fundamental in networks, and is usually achieved through encryption [8, 19, 48].

**Integrity** is the assurance that the data exchanged between two entities have not been changed during transmission, either intentionally by unauthorized entities or by accident. Necessary measures such as file permission or access control must be taken to ensure that data cannot be modified by adversaries. Control mechanisms can for instance include checksums in the data packets for integrity verification. Thus, integrity ensures the recipient of data that they have arrived in their original state. [1, 6, 9, 19, 23, 48]

**Authentication** provides a method of identifying an entity in order to ensure that the other end of a connection is the entity that is claimed [9, 19, 49]. This ensures that the data used for further processing originates from the correct source [10, 19]. Two-way authentication is an authentication in both directions, i.e., both ends of a connection authenticate to each other, ensuring that sent data originated from the claimed entity and reached only the intended entity [23].

**Authorization** is the process by which entities are equipped with rights to access services and information in the network. Usually, authorization occurs within the context of

authentication, as after an entity has authenticated it must first gain authorization to participate in the network and access or provide information. In the context of WSNs this ensures that only permitted sensors can provide information in the network. [5, 49]

**Availability** in the context of networks is the guarantee that legitimate entities can always obtain information reliably and enjoy a smooth operation of the network [1, 6, 48]. Availability is mainly targeted at Denial of Service (DoS) attacks where the network should uphold its functionality despite such attacks [9]. Measures include redundancy, use of cloud services, failover, and also appropriately maintaining hardware and software, which ensures availability in normal operation when no attack is carried out [48].

**Freshness** ensures the recipient of data that they are the most recent one [6,8]. The main purpose is to ensure no old messages are replayed by an adversary who resends previously intercepted data packets [5, 6, 8, 9, 10, 19, 23]. One distinguishes between key freshness and data freshness, where key freshness guarantees communicating entities that their key used for encryption is the newest and has not been reused [19]. The remainder of this FA will use the term freshness only if the context is clear. A measure can be, for instance, to include a nonce or some sort of time-based counter into the data packet [19].

**Non-repudiation** guarantees the recipient of a data packet that it has been sent from the correct source, i.e., it proves the source of a data packet. Thus, the sender cannot deny that he has sent the packet. A measure can be the integration of a unique signature of the sender into the data packet. [5, 9, 23]

Depending on stakeholders' requests, less or additional security fundamentals such as access control, accountability, scalability, self-organization, time synchronization or secure localization can be considered in the design of network security [1, 8, 11]. Moreover, the security fundamentals can be weighted differently according to those requests.

## 2.3 Attacks in Wireless Sensor Networks

This section introduces basic knowledge of reported attacks on WSNs based on [1, 2, 5, 8, 12, 13]. Attacks can be generally categorized based on goal, performer, layer or security fundamental [8, 12].

In **goal-oriented attacks** one distinguishes between passive and active attacks. Passive attacks are mainly directed against confidentiality where an adversary, for instance, intercepts data packets or eavesdrops on communication between two entities. In active attacks, an adversary takes active measures to gain control over the network or to impair its proper operation. Examples of active attacks include Denial of Service (DoS), Man-in-the-Middle (MITM), Sybil, impersonation, and masquerade. [8]

In a **performer-oriented categorization** one distinguishes between inside and outside attacks. In inside attacks, an adversary has managed to successfully bypass or acquire authentication and authorization, and now has legitimate nodes in the network from which attacks such as misrouting or eavesdropping can be started. In outside attacks, an adversary starts attacks outside the network without having previously obtained a security

relation with the network. Examples include passive eavesdropping of the transmission or signal jamming. [8]

Network architectures are organized in **layered forms**. WSNs typically use a simplified model of the standard OSI reference model: physical, data link, network, transport and application layer [5, 8]. Attacks can be performed on each layer and can therefore be categorized according to these layers [8]. Summarizing [5,7,8,12,13] on layered architecture and their attacks in WSNs:

- The *physical* layer is mainly responsible for selection and generation of carrier frequency, signal detection, modulation and demodulation, encryption and decryption, and data transmission. Typical attacks on this layer are jamming, tampering, node capture, node insertion, and eavesdropping.

- The *data link* layer ensures a reliable point-to-point or point-to-multipoint connection, or in the context of WSNs node-to-(multi)node. In detail, the layer multiplexes data streams, detects data frames, accesses medium and performs error control. Attacks include collision, channel and battery exhaustion, unfairness, traffic analysis, and monitoring.

- The main task of the *network* layer in WSNs is routing. In WSNs typically all nodes are responsible for routing. Moreover, data packets are routed in a hop-by-hop fashion towards a sink. This is why many attacks, especially DoS attacks, are possible on this layer: Spoofing, replay routing control messages, misdirection, flooding (HELLO and ACK), homing, wormhole, sinkhole, blackhole, selective forwarding, eavesdropping, Sybil, or Byzantine.

- The *transport* layer maintains end-to-end connections: reliability of data transmission or congestion control are typical functions of this layer. Attacks include flooding (connection requests), desynchronization, session hijacking, MITM, and impersonation.

- Providing software for various applications or responsibility of traffic management belong to the *application* layer of WSNs. Repudiation or data corruption are typical attacks on this layer.

Finally, attacks can also be **categorized after security fundamentals** introduced in Section 2.2, e.g., attacks on confidentiality, authentication, integrity or availability [12]. The Denial of Service (DoS) attacks describe a big group consisting of diverse attacks which is directed against availability [12]. In DoS attacks, adversaries attempt to disrupt or reduce expected network functionalities, or even destroy the network [13]. Since a WSN may be deployed in an open field freely accessible for adversaries—often in a critical scenario such as medical monitoring or battlefield surveillance—DoS attacks are a high risk and need to be taken care of when designing security in WSN [13]. Typical DoS attacks are jamming, tampering, collision, exhaustion, unfairness, neglect and greed, misdirection, blackhole, sinkhole, wormhole, flooding, desynchronization, and replay [2, 13]. Table 2.1 links security fundamentals introduced in Section 2.2 to selected

attacks ordered by layer [4, 5, 8, 13]. The security fundamentals are abbreviated as follows: Co = Confidentiality, In = Integrity, Ae = Authentication, Ao = Authorization, Av = Availability, Fr = Freshness, and Nr = Non-repudiation. A cross indicates that the attack can be prevented if the designer of the WSN security implements the corresponding security fundamental(s).

Table 2.1: Link table of security fundamentals and selected attacks ordered by layer

| **Layer** | **Attack** | **Co** | **In** | **Ae** | **Ao** | **Av** | **Fr** | **Nr** |
|---|---|---|---|---|---|---|---|---|
| Physical | Jamming | | | | | x | | |
| | Tampering | | x | | | | | |
| | Node capture | x | | | | | | |
| | Node insertion | | | x | x | | | |
| | Eavesdropping | x | | | | | | |
| Data Link | Collision | | | | | x | | |
| | Exhaustion | | | | | x | | |
| | Monitoring | x | | | | | | |
| Network | Spoofing | | | x | | | | |
| | Replay | | | | | | x | |
| | Misdirection | | | | x | | | |
| | HELLO flood | | | x | | | | |
| | Homing | x | | | | | | |
| | Wormhole | | | x | | | | |
| | Sinkhole | | | x | | | | |
| | Blackhole | | | | x | | | |
| | Sybil | | | x | | | | |
| Transport | Desynchronization | | | x | | | | |
| | Impersonation | | | x | | | | |
| Application | Repudiation | | | | | | | x |
| | Data corruption | | x | | | | | |

# Chapter 3

# Classification scheme

The task of this FA is to analyze the landscape of WSN-related security protocols and algorithms published in the period from 2012 to 2017, and propose a classification scheme based on the gained overview. Finally, the classification scheme is exemplarily evaluated with selected protocols and algorithms in this period by an in-depth security analysis with regard to the security fundamentals introduced in Chapter 2. The analysis and exemplary evaluation are presented in Chapter 4.

The search for journal papers in which security-related solutions for WSNs are proposed was done at Elseviers ScienceDirect [50], IEEE publication database [51], Hindawi [52], and SpringerLink [53]. The search terms were primarily "security WSN", "security wireless sensor networks", "survey security wireless sensor networks", and "security constrained networks". Surveys on security in WSNs as well as several other summarizing journal papers served as sources for security protocols and algorithms [10, 12, 14, 15, 16, 17].

Collecting over 160 journal papers in the period from 2012 to 2017 (date of publication or, if no date of publication is stated, date of acceptance by the publisher) from the aforementioned databases and surveys, and reading through their abstracts provided a sufficient overview for a classification. The broad range of security-related approaches did not allow a grouping based on specific parameters or properties, as the proposals were too diverse and often do not specify the same parameters or consider different properties. Instead, mastering the heterogeneous security approaches lead to a fine-grained subject-based classification scheme to which proposed protocols and algorithms are concerned with. Journal papers concerned with security in WSNs can be attached to several categories according to their subjects covered. The elaborated categories, derived from the over 160 collected journal papers, are listed and described from the gained overview in the following as 1 to 11.

**Category 1: Routing protocols** Nodes in a WSN are responsible for routing data packets in a network which can be very volatile in its architecture and vulnerable due to many attacks. Since nodes in many scenarios also must be self-organizing after deployment and often may be randomly deployed in a field of sensing, working out routes to a demanded end-point is a very hard task. This category presents secure routing protocols for various deployments, network architectures, mobility concepts, and attack scenarios.

**Category 2: End-to-end security** Data recorded from a sensor node has to be transmitted to an end-point where it is further processed or needed. As these data are sent in a hop-by-hop fashion and routed through several to many intermediate nodes in the WSN, confidentiality and integrity of data between the two ends—either within a single WSN or an end in the WSN and the other end outside—has to be guaranteed. Journal papers in this category are concerned with the end-to-end (E2E) security topic area.

**Category 3: Key establishment, exchange and management** In order to provide confidentiality in a network, a communication channel between entities must be secured. This is mostly done with encryption for which a key is needed. This can either be a shared secret key (symmetric encryption), or a public and private key pair (asymmetric encryption) for encryption and decryption. But keys need to be distributed first securely between entities before a secure data exchange can take place. In this category, journal papers are listed which are concerned with the secure key establishment, exchange and management.

**Category 4: Node and entity authentication** In order to establish a communication channel between nodes within a WSN or between a node inside the WSN and an entity outside the WSN, both should be sure of the counterpart's identity before data is exchanged if the security fundamental authentication is requested by stakeholders to prevent several attacks, as shown in Table 2.1. In this category are proposals of authentication schemes for the node/node and node/entity scenarios.

**Category 5: User authentication** In many scenarios an end-user is interested in the sensor data. Examples of these end-users could be professionals such as doctors interested in the medical data of their patients or security employees monitoring a facility or public places. These end-users should authenticate on nodes from which they seek sensor data, so sensitive data are not released to unauthorized users. Thus, this category is concerned with end-user authentication aspects.

**Category 6: Node registration** Depending on stakeholders' requests of self-organization, nodes must form a network on their own after initial deployment in the field of sensing. To enable this, nodes have to register on the network in order to be part of it. Moreover, in many cases it is necessary that an existing and running network is expandable by additional nodes. Such nodes also must first register in the network to extend it. This node set-up in the WSN has to be done in a secure way, such that no malicious node inserted and controlled by an adversary can participate in the network. Schemes to support this set-up process securely are in this category.

**Category 7: Data aggregation** Because WSNs are constrained in terms of bandwidth and possibly their overall lifetime, one is interested in minimizing the traffic on the network. Additionally, WSNs are data-centric, which leads to the process of data aggregation as described in Section 2.1. However, this process violates at first glance

confidentiality of data in E2E, since data has to be decrypted first in order to be able to aggregate data at intermediate nodes. This category includes schemes which provide secure data aggregation while ensuring E2E confidentiality.

**Category 8: Header compression** Classic and well-known security protocols such as DTLS or IPsec/ESP are very heavy in terms of size as they are not designed to fit constrained networks [42, 43, 44]. This can cause high traffic in a network that is constrained in possibly low bandwidth or high packet loss rate. Thus, one is interested in minimizing the headers of such protocols to be more lightweight but offering an equivalent or the same security level as the original. Proposals concerned with header compression are in this category.

**Category 9: RFID-related security** Passive RFID tags are highly constrained in computational capacity, memory and lack of power supply. Overall, this makes the use of classic security protocols and algorithms impossible for passive RFID tags. Nevertheless, very important security fundamentals such as confidentiality or authentication may be requested by stakeholders. Journal papers in this category propose tailored security protocols and algorithms for RFID.

**Category 10: New or enhanced ciphers** Well-known asymmetrical ciphers such as RSA may be too heavy for use in WSNs as they require high computational capacity, lots of memory, and produce large data packets due to long keys [3, 14, 18, 23, 45]. However, an asymmetric encryption may provide much stronger confidentiality as symmetric encryption approaches [23, 45]. In this category, journal papers are proposing new or enhanced lightweight ciphers for constrained networks.

**Category 11: Further security-related journal papers** This category comprises all journal papers that:

- Do not propose a security protocol or algorithm, but rather are general security related in WSNs (e.g., surveys, journal paper overviews, attacks overview, new possible attacks)
- Propose a security solution for a too specific real-world scenario
- Only look at a very detailed security issue and propose a solution for it
- Are in total too few on a same security-related subject in WSNs
- Propose only an approach which is too generally formulated

# Chapter 4

# Analysis

This chapter provides an exemplary evaluation of the proposed subject-based classification scheme introduced in Chapter 3, which was derived from over 160 collected journal papers in the period from 2012 and 2017. The evaluation is done through an in-depth security analysis of selected protocols and algorithms from the collected journal papers, with regard to the security fundamentals introduced in Chapter 2. Finally, the elaborated results are presented in a comparative table at the end of this chapter. The evaluation is done exemplarily for the categories 1 to 4, i.e., "Routing protocols", "End-to-end security", "Key establishment, exchange and management", and "Node and entity authentication", since this FA is limited in time and scope, and these categories are four of the most important subjects on security in WSNs and therefore provide many journal papers. Each category has four proposals from different journal papers to ensure the number of representatives of the categories is balanced.

The journal papers with security-related proposals in the aforementioned categories were almost randomly selected so that they are interchangeable. In the first place, they serve to provide an exemplary evaluation rather than an overview of security protocols and algorithms between 2012 and 2017. The proposals from journal papers [32] (PAuthKey) and [25] (TinyDTLS), as well as from a book chapter in [3] (TinyTO) were mandatory by the supervisor Corinna Schmitt as they were developed or co-developed by her.

Note that some categories are not concerned with all security fundamentals introduced in Section 2.2. For instance, the category "Node and entity authentication" is only concerned with authentication. This is because other security fundamentals are not implemented by this category. Moreover, proposed protocols or algorithms in journal papers can cover several categories, e.g., "End-to-end security", "Node and entity authentication" as well as "User authentication". However, this is discussed individually at appropriate points in the following sections or in the analysis of the individual protocols and algorithms.

The following **assumptions** were made in the analysis of the 16 algorithms and protocols regarding the security fundamentals:

- As explained in Section 2.2, and showed in Table 2.1, an encryption as well as a proof of resistance against eavesdropping attacks always provides **confidentiality**.

- A Message Authentication Code (MAC) included in the data packet guarantees that the proposal ensures **integrity** [30].
- Asymmetric cryptosystems provide **authentication** in a natural way through the private and public key pair. This is because the decryption of a received message can only be successful when the message was encrypted by the sender, since his key is private [20].
- As mentioned in Section 2.2, a data cloud or redundancy in the network implies that the security fundamental **availability** is given. Moreover, as explained in the same section, if the proposal is to be proven generally resistant against DoS attacks, it also ensures availability.
- Section 2.2 linked the resistance against replay attacks with the guarantee of **freshness** (data or key depending on the context). Also mentioned in the same section, a nonce or a time-based counter included in the data packet also ensures freshness. Moreover, the use of a unique sequence number in data packets guarantees freshness as well [23].
- A unique signature added in data packets prevents repudiation, thus, guarantees **non-repudiation**, when included in the data packet as mentioned in Section 2.2.

In Sections 4.1 to 4.4 follows the detailed security analysis of selected protocols and algorithms. Table 4.1 summarizes these results in a comparative table. In this table, the year refers to the date of publication or the date of acceptance by the publisher if the date of publication is not stated. "Cat" refers to the main category to which the proposal is concerned, and "Ad Cat" lists all additional categories to which the proposal is also concerned. "Ad Cat" can be empty, meaning that the journal paper is only concerned with the main category. The abbreviations used in the table for the categories introduced in Chapter 3 are as follows: R = Routing protocols, E2E = End-to-end security, K = Key establishment, management and exchange, NA = Node and entity authentication, U = User authentication, NR = Node registration, and A = Data aggregation. The security fundamentals introduced in Section 2.2 are abbreviated as follows: Co = Confidentiality, In = Integrity, Ae = Authentication, Ao = Authorization, Av = Availability, Fr = Freshness, and Nr = Non-repudiation. Finally, following symbols were used in the table: "y" means the security fundamental is supported by the proposal, "n" means the security fundamental is not supported by the proposal, an empty cell means that no statement is made in the journal paper or no clear derivation could be made with the assumptions concerning the security fundamental (i.e., an empty cell means N/A), and "–" means that the security fundamental is not applicable in the category or in the proposal.

## 4.1 Category 1: Routing protocols

In [20], a digital signature-based multipath routing protocol called **EENDMRP** (Energy Efficient Node Disjoint Multipath Routing Protocol) is proposed. Confidentiality is

ensured through the use of the digital signature cryptosystem. This cryptosystem uses the MD5 hash function to generate digital signatures and the RSA algorithm to generate private and public key pairs. The use of this cryptosystem also ensures authentication, integrity and non-repudiation.

[21] proposes a secure routing protocol called **SR3** (Secure Resilient Reputation-based Routing), which is designed as a reinforced random walk. Confidentiality is guaranteed through the use of symmetric encryption. Integrity is ensured by the comparison of the hash of a nonce. The use of nonces in data packets should furthermore guarantee freshness. Hash functions and nonces are also used in the proposed protocol to determine the message's authenticity, providing thus authentication.

In [22], a secure location-aware geographic routing scheme based on received signal strength for flat WSNs is proposed, called **SGOR** (Secure and Scalable Geographic Opportunistic Routing). Confidentiality is ensured through symmetric encryption. Integrity is ensured by the protocol because nodes which have sent a packet afterwards listen to the channel in order to intercept the same packet when the next nodes forward it to their next hop nodes, and check if the packet somehow has been modified. The authentication is done indirectly with the comparison of known location and received signal strength of the node's neighborhood nodes. This process verifies the authenticity of nodes. Availability is given as the protocol implements redundancy through multicast routing. Freshness should be given because it uses timestamps and is secure against replay attacks.

[23] proposes Secure Hierarchical and Role based Routing Protocol (**SHaRP**) in which the focus lies on the routing process in WSNs. But the proposed framework also includes node registration and authentication, covering thus the categories "Node and entity authentication" and "Node registration". The protocol therefore implements authentication. Moreover, the proposal includes key establishment and management functionalities as well as secure data aggregation at cluster heads. Therefore, SHaRP covers also the categories "Key establishment, exchange and management" and "Data aggregation". SHaRP ensures confidentiality through encryption with a combination of symmetric and asymmetric cryptography. Integrity is ensured through the use of MAC. Availability is ensured because the authors proved that their framework is resistant against DoS attacks. Data as well as key freshness is guaranteed by the use of a unique sequence number and periodic key refreshing respectively. A unique signature integrated in each data packet ensures non-repudiation.

## 4.2 Category 2: End-to-end security

Three of the selected four proposals in this group implement the Datagram Transport Layer Security (DTLS) protocol in the transport layer, which is based on TLS to guarantee a secure E2E communication in the IoT context. The fourth proposal relies on the DTLS protocol. DTLS is a handshake protocol, that is, the keys for encryption as well as the cryptosystem is negotiated between two entities—in the case of DTLS between server and client. Thus, DTLS guarantees in any case confidentiality as it defines the encryption for the upcoming communication. Moreover, DTLS uses MAC in data packets ensuring also

integrity in any case. DTLS offers three types of handshakes: unauthenticated (no entity authenticates during handshake to each other), server side authenticated (only the server authenticates to clients), and fully authenticated handshake (both entities authenticate each other). However, all four examined proposals do not consider the unauthenticated case, making all four ensuring authentication as well. [25, 27, 47]

Thus, checking the proposals for authorization, availability, freshness and non-repudiation still remain. Although DTLS offers mechanism to defend replay attacks and thus, would also ensure freshness, it is optional [47].

In [24], an architecture for E2E transport layer security in IoT is proposed. The architecture is called **ME2ECoAP** (Mediated E2E CoAP) and implements DTLS. It is based on mutual authentication using Elliptic Curve Cryptography (ECC), which is an instance of asymmetric cryptography. An Access Control server included in the architecture provides authorization. The use of timestamps guarantees resistance against replay attacks and thus, ensures freshness.

[25] proposes a two-way authentication scheme called **TinyDTLS** in the IoT context, which implements DTLS. The paper's focus is on secure E2E communication by using a scheme based on the RSA cryptosystem. TinyDTLS implements the fully authenticated DTLS handshake. Authorization is given through the use of an Access Control server as a trusted entity. The authors explicitly rely on other schemes to guarantee availability, meaning availability is not ensured by the proposal.

In [26], an architecture for E2E security in IoT called **OSCAR** (Object SeCurity ARchitecture) is proposed. The architecture does not implement DTLS, but rather assumes that an authenticated DTLS connection is already established. OSCAR uses keys for encryption derived from Access Secrets which are provided by Authorization Servers. Thus, authorization is given through these servers. Availability is indirectly given because the architecture includes a cloud or in-network proxy servers. Freshness is ensured in OSCAR because the authors suggest updating Access Secrets over time so used message IDs do not wrap up. This causes the architecture to be resistant against replay attacks. The use of digital signatures ensures non-repudiation.

[27] implements DTLS again based on AES and ECC. It proposes an architecture for a secure E2E communication called **SecureSense** in which CoAP is used as an application layer. Availability is indirectly given through the integration of a cloud. The use of an ECC signature should guarantee non-repudiation.

## 4.3 Category 3: Key establishment, exchange and management

In this category, the context of the security fundamentals refers to keys instead of data, i.e., key confidentiality, key integrity, key freshness, and authentication refers to authenticated key exchange. The security fundamentals authorization, availability and non-repudiation are not applicable in this category as it is not concerned with these security aspects.

[28] proposes a distributed key exchange scheme for the Host Identity Protocol (HIP) in the context of IoT, called **D-HIP**. It presents a scheme which offers the same security as HIP but distributes the heavy cryptographic computation to less constrained nodes in the neighborhood. As it only modifies HIP, confidentiality and integrity should still be ensured, and HIP Base Exchange provides authentication. Key freshness is given through the use of MAC.

[29] proposes an identity-based key management (**IBKM**) scheme for hierarchical WSNs. The scheme also includes registration of nodes at the cluster head, covering thus the category "Node registration". Moreover, IBKM describes authentication between nodes using the Bloom filter. Therefore, the scheme covers also the category "Node and entity authentication" and ensures authentication. The scheme implements an identity-based cryptosystem to establish session keys between nodes for an upcoming communication. Thus, confidentiality is ensured. Freshness should be given through the use of timestamps.

In [30], a key establishment protocol for WSNs called **DKEP** (Disjoint Key Establishment Protocol) is proposed. Each node is preloaded with a row and a column from a matrix. After deployment, the indices of the preloaded row and column are exchanged between two nodes which need to communicate. The symmetric key is then derived from the matrix entries corresponding to the exchanged indices at both nodes simultaneously. This method ensures confidentiality because only indices are transmitted and the key then calculated at the nodes. Integrity is ensured through the use of MAC. The authors use Ruben Logic to verify authentication. The use of timestamps furthermore guarantees freshness.

[31] proposes a key establishment scheme in the IoT context to enable running the DTLS protocol on devices that have no previous security relationship with a server. The framework is called **S3K** (Scalable Security with Symmetric Keys) and comprises two schemes to establish a security relation between entities. The key establishment builds on a Trust Anchor from which keys can be received such that the public key's integrity as well as the private key's confidentiality and integrity is guaranteed. Key freshness is guaranteed by the use of a sequence number to mark already used keys.

## 4.4 Category 4: Node and entity authentication

This category alone only serves and provides authentication, because all other security fundamentals are not covered by this category. But most of the proposals do not focus only on "Node and entity authentication", although this category is their main focus. Thus, proposals in this category have ensured authentication and depending on other security subjects they might cover, additional categories can be attached and therefore additional security fundamentals are also possible.

[32] proposes an authentication scheme in the IoT context called **PAuthKey** (Pervasive Authentication and Key), which considers authentication not only between different entities inside and outside a WSN, but also end-user authentication, covering therefore also the category "User authentication". Moreover, the proposal includes a key establishment scheme and provides a node registration phase. Thus, the scheme also covers

the categories "Key establishment, exchange and management" and "Node registration". PAuthKey builds upon an existing secure DTLS connection. Hence, integrity and confidentiality are ensured, as mentioned in Section 4.2. As DTLS provides E2E security, PAuthKey covers also the category "End-to-end security". The protocol uses external Certificate Authorities ensuring availability of the scheme. Also, the certificates provide non-repudiation. Freshness is given through a random cryptographic nonce.

[33] proposes an Authentication and Key Management Scheme (**AKMS**) for WSNs. Thus, as in Section 4.3 mentioned, authorization, availability and non-repudiation are not considered in the category "Key establishment, exchange and management". But authentication is guaranteed in the category "Node and entity authentication". A network initialization phase in AKMS covers also the category "Node registration". The proposal uses symmetric cryptographic primitives, ensuring confidentiality. Included MAC guarantees integrity. Freshness is given as the scheme is proven to be resistant against replay attacks.

In [34], a watermark-based node authentication scheme called **LoWaNA** (Low overhead Watermark-based Node Authentication) for flat WSNs is proposed. As this paper focus only on authentication, it provides no other security fundamentals as mentioned at the beginning of this section.

In [3], **TinyTO** is proposed, a two-way authentication scheme for IoT-based constrained devices. The authors take also E2E security into consideration by using ECC, covering thus additionally the category "End-to-end security" and ensuring confidentiality. The proposal provides integrity as well. Moreover, it is proven that the scheme is resistant to replay attacks, yielding freshness. ECC is moreover responsible to generate signatures which ensures non-repudiation.

Table 4.1: Analysis and grouping table for classification scheme

| Cat | Proposal | Year | Ad Cat | Co | In | Ae | Ao | Av | Fr | Nr |
|---|---|---|---|---|---|---|---|---|---|---|
| R | EENDMRP [20] | 2012 | | y | y | y | | | | y |
| | SR3 [21] | 2013 | | y | y | y | | | y | |
| | SGOR [22] | 2015 | | y | y | y | | y | y | |
| | SHaRP [23] | 2016 | K/NA/NR/A | y | y | y | | y | y | y |
| E2E | ME2ECoAP [24] | 2013 | | y | y | y | y | | y | |
| | TinyDTLS [25] | 2013 | | y | y | y | y | n | | |
| | OSCAR [26] | 2014 | | y | y | y | y | y | y | y |
| | SecureSense [27] | 2017 | | y | y | y | | y | | y |
| K | D-HIP [28] | 2012 | | y | y | y | – | – | y | – |
| | IBKM [29] | 2014 | NA/NR | y | | y | – | – | y | – |
| | DKEP [30] | 2016 | | y | y | y | – | – | y | – |
| | S3K [31] | 2016 | | y | y | | – | – | y | – |
| NA | PAuthKey [32] | 2014 | E2E/K/U/NR | y | y | y | | y | y | y |
| | AKMS [33] | 2016 | K/NR | y | y | y | – | – | y | – |
| | LoWaNA [34] | 2016 | | – | – | y | – | – | – | – |
| | TinyTO [3] | 2016 | E2E | y | y | y | | | y | y |

# Chapter 5

# Conclusion

This FA proposed a quantitative, not exclusive, subject-based classification scheme of journal papers which are concerned with security-related issues in WSNs. The classification scheme was derived from over 160 researched journal papers in the period from 2012 to 2017. The broad landscape of security-related approaches in WSNs—as the collected journal papers showed—lead to a fine-grained subject-based classification scheme with 11 categories. The derivation of the scheme from the collected journal papers ensures a complete and as detailed as possible classification of these journal papers by allowing a journal paper to cover more than one category. The scheme was elaborated in such a way that it remains open for further security-related journal papers on WSNs and for future developments in the area of security in WSNs. Subsequently, the scheme was exemplarily evaluated with selected 16 protocols and algorithms from the collected journal papers from four different categories as their main category by an in-depth security analysis with regard to well-known security fundamentals, which were introduced and defined in Chapter 2. The exemplary evaluation implies the necessary fineness, and the universal adaptability of the proposed classification.

The classification scheme can be seen as a kit for developers what to implement depending on the requirements of a specific WSN and stakeholders' requests when designing security in a WSN, an evaluation and comparison tool for different protocols and algorithms when implementing security functions in a WSN, or can give a quantitative classified overview of the broad landscape of security-related approaches in WSNs. Also, it can be a basis for a more comprehensive future work as this FA was limited in time and scope.

# Bibliography


[1] Holger Karl, Andreas Willig: Protocols and Architectures for Wireless Sensor Networks, John Wiley & Sons Ltd, April 2005, ISBN 978-0-470-09510-2.

[2] D.P. Acharjya, M. Kalaiselvi Geetha: Internet of Things: Novel Advances and Envisioned Applications, Springer International Publishing AG, April 2017, ISBN 978-3-319-53470-1, DOI: 10.1007/978-3-319-53472-5.

[3] Rajkumar Buyya, Amir Vahid Dastjerdi: Internet of Things – Principles and Paradigms, Elsevier Inc., May 2016, ISBN 978-0-12-805395-9, DOI: 10.1016/B978-0-12-805395-9.00019-8.

[4] Henk C.A. van Tilborg: Encyclopedia of Cryptography and Security, Springer US, September 2005, ISBN 978-0-387-23473-1, DOI: 10.1007/0-387-23483-7.

[5] Yong Wang, Garhan Attebury, Byrav Ramamurthy: A Survey of Security Issues in Wireless Sensor Networks, Institute of Electrical and Electronics Engineers (IEEE), 2006, ISSN 1553-877X, DOI: 10.1109/COMST.2006.315852.

[6] Qiuwei Yang, Xiaogang Zhu, Hongjuan Fu, Xiqiang Che: Survey of Security Technologies on Wireless Sensor Networks, Hindawi Publishing Corporation, December 2014, ISSN 1687-7268, DOI: 10.1155/2015/842392.

[7] Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, Erdal Cayirci: A Survey on Sensor Networks, Institute of Electrical and Electronics Engineers (IEEE), November 2002, ISSN 0163-6804, DOI: 10.1109/MCOM.2002.1024422.

[8] Kahina Chelli: Security Issues in Wireless Sensor Networks: Attacks and Countermeasures, International Association of Engineers, April 2015, ISSN 2078-0966.

[9] Asmae Blilat, Anas Bouayad, Nour El Houda Chaoui, Mohammed El Ghazi: Wireless sensor network: Security challenges, Institute of Electrical and Electronics Engineers (IEEE), July 2012, ISBN 978-1-4673-1052-9, DOI: 10.1109/JNS2.2012.6249244.

[10] Kim Thuat Nguyen, Maryline Laurent, Nouha Oualha: Survey on secure communication protocols for the Internet of Things, Elsevier B.V., February 2015, ISSN 1570-8705, DOI: 10.1016/j.adhoc.2015.01.006.

[11] David W. Carman, Peter S. Kruus, Brian J. Matt: Constraints and approaches for distributed sensor network security, Network Associates Inc., September 2000.

[12] Tuhin Borgohain, Uday Kumar, Sugata Sanyal: Survey of Security and Privacy Issues of Internet of Things, Cornell University Library, January 2015, arXiv: 1501.02211.

[13] Anthony D. Wood, John A. Stankovic: Denial of Service in Sensor Networks, Institute of Electrical and Electronics Engineers (IEEE), December 2002, ISSN 0018-9162, DOI: 10.1109/MC.2002.1039518.

[14] Saurabh Singh, Pradip Kumar Sharma, Seo Yeon Moon, Jong Hyuk Park: Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions, Springer Berlin Heidelberg, May 2017, ISSN 1868-5145, DOI: 10.1007/s12652-017-0494-4.

[15] Fadele Ayotunde Alaba, Mazliza Othman, Ibrahim Abaker Targio Hashem, Faiz Alotaibi: Internet of Things security: A survey, Elsevier Ltd., April 2017, ISSN 1084-8045, DOI: 10.1016/j.jnca.2017.04.002.

[16] Shazana Md Zin, Nor Badrul Anuar, Miss Laiha Mat Kiah, Al-Sakib Khan Pathan: Routing protocol design for secure WSN: Review and open research issues, Elsevier Ltd., March 2014, ISSN 1084-8045, DOI: 10.1016/j.jnca.2014.02.008.

[17] Fei Yu, Chin-Chen Chang, Jian Shu, Iftikhar Ahmad, Jun Zhang, Jose Maria de Fuentes: Recent Advances in Security and Privacy for Wireless Sensor Networks 2016, Hindawi Publishing Corporation, February 2017, ISSN 1687-7268, DOI: 10.1155/2017/3057534.

[18] Jaydip Sen: A Survey on Wireless Sensor Network Security, Cornell University Library, August 2009, arXiv: 1011.1529.

[19] John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhary: Wireless Sensor Network Security: A Survey, Auerbach Publications, March 2007, ISBN 978-0-8493-7921-5.

[20] Shiva Murthy G, Robert John D'Souza, Golla Varaprasad: Digital Signature-Based Secure Node Disjoint Multipath Routing Protocol for Wireless Sensor Networks, Institute of Electrical and Electronics Engineers (IEEE), June 2012, ISSN 1558-1748, DOI: 10.1109/JSEN.2012.2205674.

[21] Karine Altisen, Stéphane Devismes, Raphaël Jamet, Pascal Lafourcade: SR3: Secure Resilient Reputation-based Routing, Institute of Electrical and Electronics Engineers (IEEE), July 2013, ISSN 2325-2944, DOI: 10.1109/DCOSS.2013.33.

[22] Chen Lyu, Dawu Gu, Xiaomei Zhang, Shifeng Sun, Yuanyuan Zhang, Amit Pande: SGOR: Secure and scalable geographic opportunistic routing with received signal strength in WSNs, Elsevier B.V., January 2015, ISSN 0140-3664, DOI: 10.1016/j.comcom.2015.01.003.

[23] Hiren Kumar Deva Sarma, Avijit Kar, Rajib Mall: A Hierarchical and Role Based Secure Routing Protocol for Mobile Wireless Sensor Networks, Springer US, June 2016, ISSN 1572-834X, DOI: 10.1007/s11277-016-3379-5.

[24] Jorge Granjal, Edmundo Monteiro, Jorge Sá Silva: End-to-end transport-layer security for Internet-integrated sensing applications with mutual and delegated ECC public-key authentication, Institute of Electrical and Electronics Engineers (IEEE), November 2013, ISBN 978-3-901882-55-5.

[25] Thomas Kothmayr, Corinna Schmitt, Wen Hub, Michael Brünig, Georg Carle: DTLS based security and two-way authentication for the Internet of Things, Elsevier B.V., May 2013, ISSN 1570-8705, DOI: 10.1016/j.adhoc.2013.05.003.

[26] Mališa Vučinić, Bernard Tourancheau, Franck Rousseau, Andrzej Duda, Laurent Damon, Roberto Guizzetti: OSCAR: Object security architecture for the Internet of Things, Elsevier B.V., December 2014, ISSN 1570-8705, DOI: 10.1016/j.adhoc.2014.12.005.

[27] Shahid Raza, Tómas Helgason, Panos Papadimitratos, Thiemo Voigt: SecureSense: End-to-end secure communication architecture for the cloud-connected Internet of Things, Elsevier B.V., June 2017, ISSN 0167-739X, DOI: 10.1016/j.future.2017.06.008.

[28] Yosra Ben Saied, Alexis Olivereau: D-HIP: A distributed key exchange scheme for HIP-based Internet of Things, Institute of Electrical and Electronics Engineers (IEEE), August 2012, ISBN 978-1-4673-1237-0, DOI: 10.1109/WoWMoM.2012.6263785.

[29] Zhongyuan Qin, Xinshuai Zhang, Kerong Feng, Qunfang Zhang, Jie Huang: An efficient identity-based key management scheme for wireless sensor networks using the Bloom filter, Multidisciplinary Digital Publishing Institute (MDPI), September 2014, ISSN 1424-8220, DOI: 10.3390/s141017937.

[30] AtaUllah Ghafoor, Muhammad Sher, Muhammad Imran, Imran Baig: Disjoint Key Establishment Protocol for Wireless Sensor and Actor Networks, Hindawi Publishing Corporation, May 2016, ISSN 1687-7268, DOI: 10.1155/2016/5071617.

[31] Shahid Raza, Ludwig Seitz, Denis Sitenkov, and Göran Selander: S3K: Scalable Security With Symmetric Keys—DTLS Key Establishment for the Internet of Things, Institute of Electrical and Electronics Engineers (IEEE), January 2016, ISSN 1558-3783, DOI: 10.1109/TASE.2015.2511301.

[32] Pawani Porambage, Corinna Schmitt, Pardeep Kumar, Andrei Gurtov, Mika Ylianttila: PAuthKey: A Pervasive Authentication Protocol and Key Establishment Scheme for Wireless Sensor Networks in Distributed IoT Applications, Hindawi Publishing Corporation, July 2014, ISSN 1550-1477, DOI: 10.1155/2014/357430.

[33] Danyang Qin, Shuang Jia, Songxiang Yang, ErfuWang, Qun Ding: A Lightweight Authentication and Key Management Scheme for Wireless Sensor Networks, Hindawi Publishing Corporation, September 2016, ISSN 1687-7268, DOI: 10.1155/2016/1547963.

[34] Arpan Sen, Tanusree Chatterjee, Sipra DasBit: LoWaNA: low overhead watermark based node authentication in WSN, Springer US, January 2016, ISSN 1572-8196, DOI: 10.1007/s11276-015-1157-z.

[35] Kakali Chatterjee, Asok De, Daya Gupta: A Secure and Efficient Authentication Protocol in Wireless Sensor Network, Springer US, October 2014, ISSN 1572-834X, DOI: 10.1007/s11277-014-2115-2.

[36] Ashok Kumar Das, Pranay Sharma, Santanu Chatterjee, Jamuna Kanta Sing: A dynamic password-based user authentication scheme for hierarchical wireless sensor networks, Elsevier Ltd., April 2012, ISSN 1084-8045, DOI: 10.1016/j.jnca.2012.03.011.

[37] Shipra Kumari, Hari Om: Authentication protocol for wireless sensor networks applications like safety monitoring in coal mines, Elsevier B.V., May 2016, ISSN 1389-1286, DOI: 10.1016/j.comnet.2016.05.007, URL: https://doi.org/10.1016/j.comnet.2016.05.007.

[38] Prerna Mohit, Ruhul Amin, G.P. Biswas: Design of authentication protocol for wireless sensor network-based smart vehicular system, Elsevier Inc., March 2017, ISSN 2214-2096, DOI: 10.1016/j.vehcom.2017.02.006.

[39] Mohammed Riyadh Abdmeziem, Djamel Tandjaoui: An end-to-end secure key management protocol for e-health applications, Elsevier Ltd., April 2015, ISSN 0045-7906, DOI: 10.1016/j.compeleceng.2015.03.030.

[40] Debiao He, Neeraj Kumar, Jianhua Chen, Cheng-Chi Lee, Naveen Chilamkurti, Seng-Soo Yeo: Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks, Springer Berlin Heidelberg, December 2013, ISSN 1432-1882, DOI: 10.1007/s00530-013-0346-9.

[41] Chunyan Peng, Xiujuan Du, Keqin Li, Meiju Li: An Ultra-Lightweight Encryption Scheme in Underwater Acoustic Networks, Hindawi Publishing Corporation, February 2016, ISSN 1687-7268, DOI: 10.1155/2016/8763528.

[42] Shahid Raza, Hossein Shafagh, Kasun Hewage, René Hummen, Thiemo Voigt: Lithe: Lightweight Secure CoAP for the Internet of Things, Institute of Electrical and Electronics Engineers (IEEE), August 2013, ISSN 1558-1748, DOI: 10.1109/JSEN.2013.2277656.

[43] Shahid Raza, Daniele Trabalza, Thiemo Voigt: 6LoWPAN Compressed DTLS for CoAP, Institute of Electrical and Electronics Engineers (IEEE), July 2012, ISBN 978-0-7695-4707-7, DOI: 10.1109/DCOSS.2012.55.

[44] D. Migault, T. Guggemos, C. Bormann: Diet-ESP: a flexible and compressed format for IPsec/ESP (Internet-Draft, work in progress), Internet Engineering Task Force (IETF), July 2016, URL: https://tools.ietf.org/html/draft-mglt-6lo-diet-esp-02 (last visit August 24, 2017).

[45] Qiang Zhou, Geng Yang, Liwen He: A Secure-Enhanced Data Aggregation Based on ECC in Wireless Sensor Networks, Multidisciplinary Digital Publishing Institute (MDPI), April 2014, ISSN 1424-8220, DOI: 10.3390/s140406701.

[46] C. Bormann, M. Ersue, A. Keranen: RFC 7228: Terminology for Constrained-Node Networks, Internet Engineering Task Force (IETF), May 2014, ISSN 2070-1721, DOI: 10.17487/RFC7228.

[47] E. Rescorla, N. Modadugu: RFC 6347: Datagram Transport Layer Security Version 1.2, Internet Engineering Task Force (IETF), January 2012, ISSN 2070-1721, DOI: 10.17487/RFC6347.

[48] http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA (last visit August 23, 2017).

[49] http://searchsecurity.techtarget.com/definition/authentication-authorization-and-accounting (last visit August 23, 2017).

[50] http://www.sciencedirect.com/ (last visit August 23, 2017).

[51] http://ieeexplore.ieee.org/ (last visit August 23, 2017).

[52] https://www.hindawi.com/ (last visit August 23, 2017).

[53] https://link.springer.com/ (last visit August 23, 2017).

# Abbreviations

| | |
|---|---|
| Ae | Authentication |
| AES | Advanced Encryption Standard |
| Ao | Authorization |
| Av | Availability |
| Co | Confidentiality |
| CoAP | Constrained Application Protocol |
| DoS | Denial of Service |
| DTLS | Datagram Transport Layer Security |
| ECC | Elliptic Curve Cryptography |
| ESP | Encapsulated Security Payload |
| FA | Facharbeit |
| Fr | Freshness |
| HIP | Host Identity Protocol |
| ID | Identifier |
| IEEE | Institute of Electrical and Electronics Engineers |
| In | Integrity |
| IP | Internet Protocol |
| IPsec | Internet Protocol Security |
| MAC | Message Authentication Code |
| MD5 | Message Digest 5 |
| MITM | Man-in-the-Middle |
| Nr | Non-repudiation |
| OSI | Open Systems Interconnection |
| RFID | Radio-frequency identification |
| RSA | Rivest, Shamir and Adleman cryptosystem |
| TCP | Transmission Control Protocol |
| TLS | Transport Layer Security |
| WLAN | Wireless Local Area Network |
| WSAN | Wireless Sensor and Actuator Network |
| WSN | Wireless Sensor Network |

# List of Tables

# Appendix A

# Contents of the CD

The following is a view of the folder structure and contents.

- **Presentation**: Contains the presentation of this FA in file formats pptx and pdf
- **References**: Contains all references used in this report in file format pdf with file name {reference number}.pdf
- **Report**
  - **PDF**: Contains this report in file format pdf
  - **TeX**: Contains this report as TEX file collection