HSB
Hochschule Bremen
City University of Applied Sciences

Custom Transport Interface for the Integration of Trusted Network Connect in German Smart Metering Systems

Carl-Heinz Genzel, Richard Sethmann

University of Applied Sciences Bremen, Flughafenallee 10, 28199 Bremen, Germany

Inhalt

1. Introduction
2. Smart Metering Systems
3. Integrity Protection and Monitoring
4. Data Transport
5. Evaluation
6. Conclusion & Prospects

INTRODUCTION

Introduction

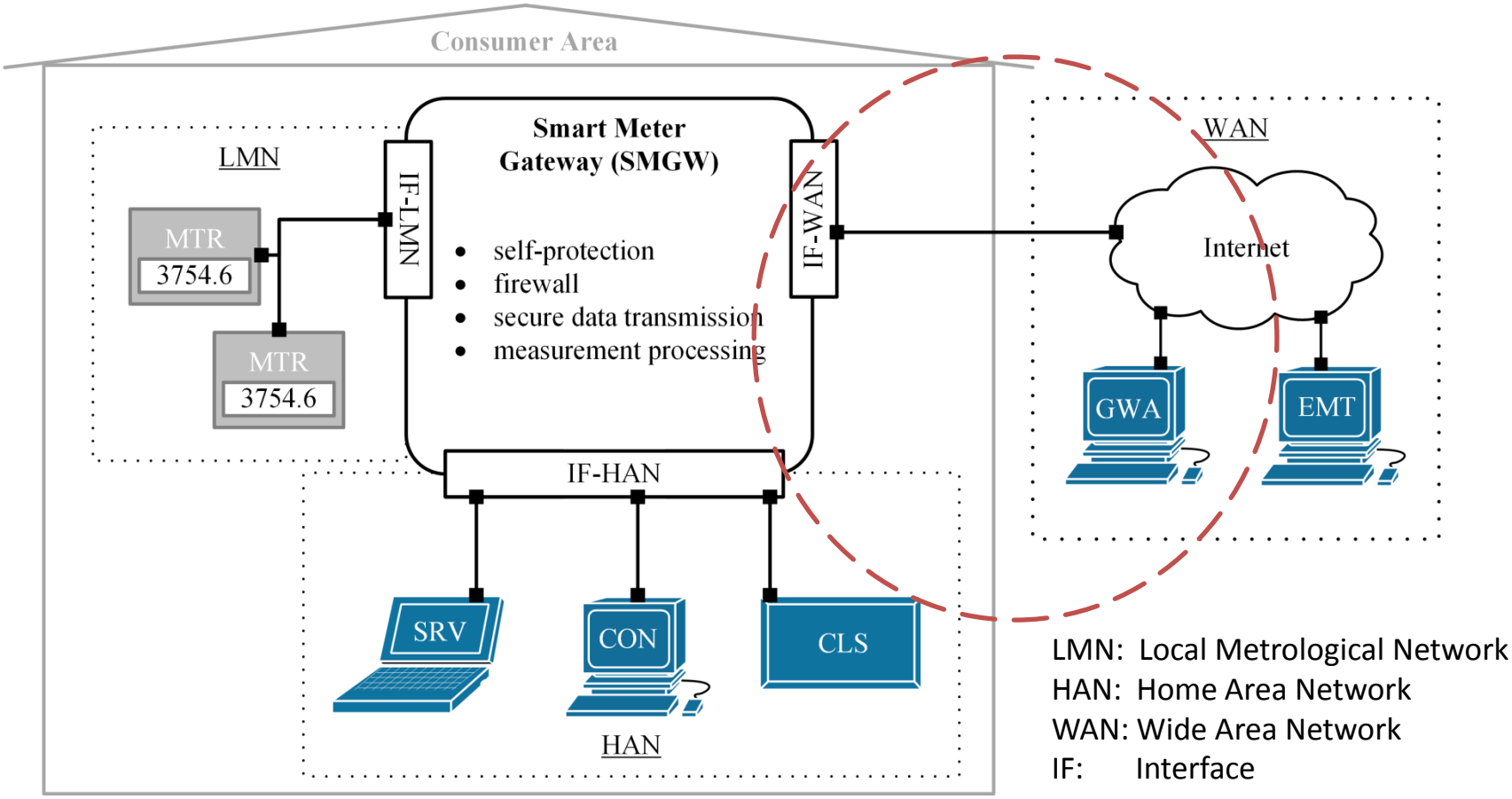
- Introduction of Smart Metering Systems by the German government
- Security architecture for Smart Metering Systems developed by the Federal Office for Information Security (BSI)
- Research project SPIDER
  - Analysis of the security architecture revealed that the integrity of a major component may be vulnerable
  - Trusted Network Connect (TNC) specified by the Trusted Computing Group (TCG) for integrity monitoring

Introduction

- Main tasks for this paper:
  - Evaluation of the existing specifications
    - BSI specifications for the Smart Metering System
    - TCG specifications for the Trusted Network Connect architecture
  - Development of solutions to overcome contradictions between the existing specifications
  - Evaluation of the developed solutions

SMART METERING SYSTEM

Smart Metering Systems



LMN: Local Metrological Network
HAN: Home Area Network
WAN: Wide Area Network
IF: Interface

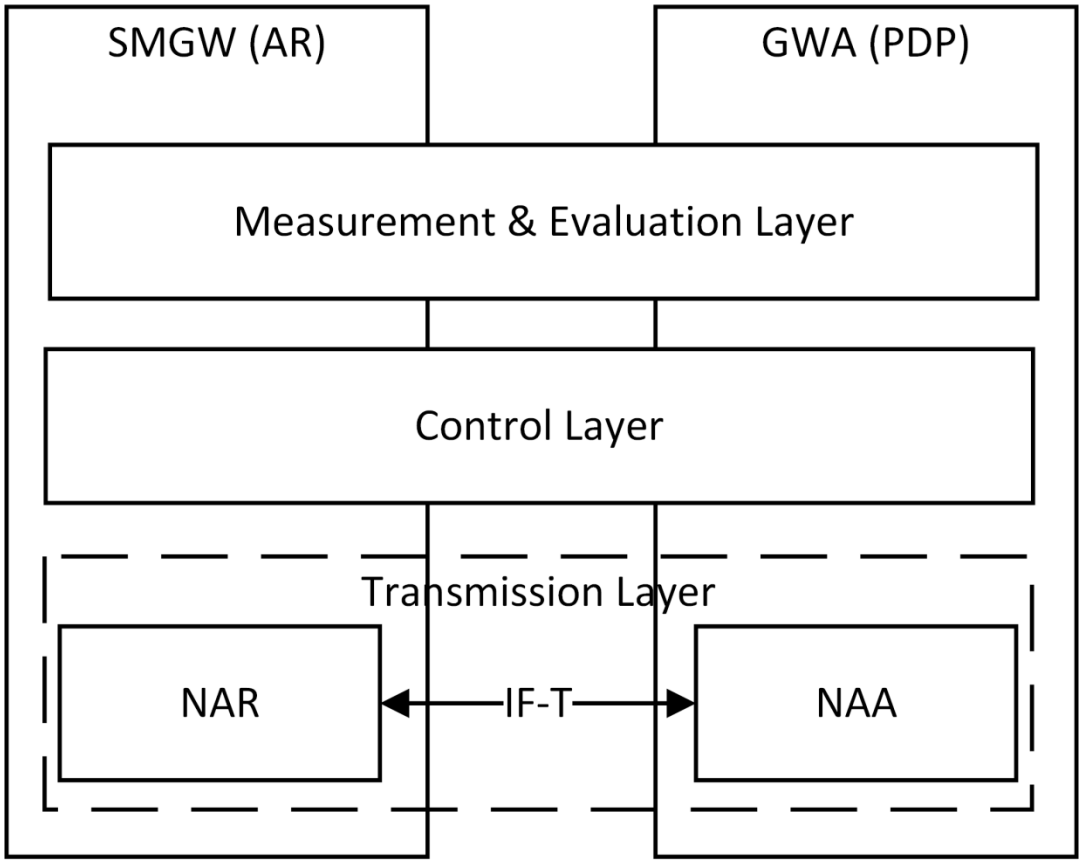
MTR: Smart Meter SRV: Service Technician CON: Consumer CLS: Controllable Local System
GWA: Gateway Administrator EMT: Authorized External Entity

INTEGRITY PROTECTION AND MONITORING

Integrity Protection and Monitoring: Concept

- Hardware protection
  - Visible permanent seal, housing state detection, tamper resistant grid
- Boottime protection
  - Secure Boot-Pattern
- Runtime protection
  - Remote Attestation using TNC
    - Continuously measurement of the systems integrity state
    - Assessment of the systems integrity by a remote instance using the measured system integrity state

Integrity Protection and Monitoring: TNC



DATA TRANSPORT

Data Transport: TCG IF-T

- Interface depends on physical connection and its lower layer protocols
- Separate specifications for different connection types
  - TCG Trusted Network Connect TNC IF-T: Protocol Bindings for Tunneled EAP Methods (IF-T-EAP)
    - Integrity state as part of an authentication to access a network (e. g. 802.1x)
  - TCG Trusted Network Connect TNC IF-T: Binding to TLS (IF-T-TLS)
    - Integrity state as part of a continuous system monitoring through an existing connection to a network

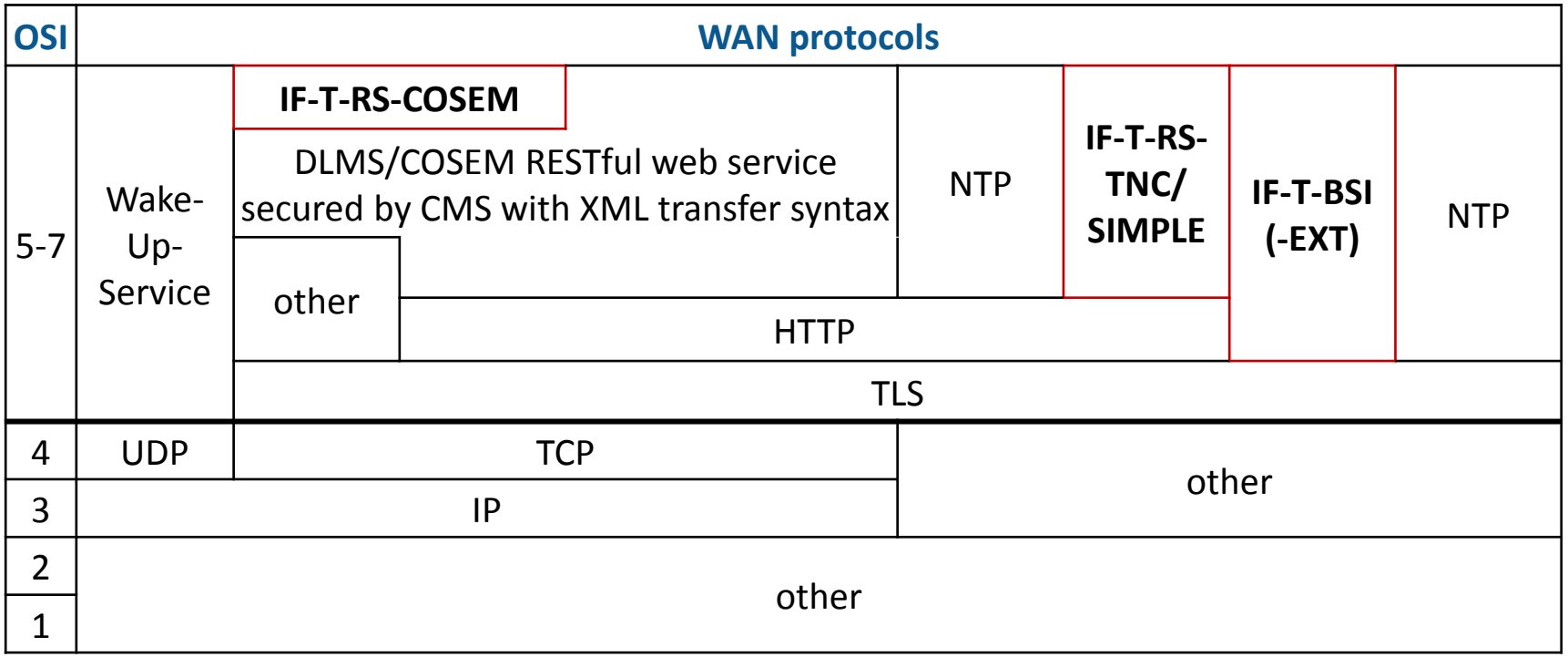
Data Transport: BSI IF-WAN

<table>
<tr><th>OSI</th><th colspan="5">WAN protocols</th></tr>
<tr><td rowspan="3">5-7</td><td rowspan="3">Wake-Up-Service</td><td colspan="2">DLMS/COSEM RESTful web service secured by CMS with XML transfer syntax</td><td>NTP</td><td>other</td><td rowspan="2">NTP</td></tr>
<tr><td rowspan="2">other</td><td colspan="2">HTTP</td></tr>
<tr><td colspan="4">TLS</td></tr>
<tr><td>4</td><td>UDP</td><td colspan="2">TCP</td><td colspan="2" rowspan="2">other</td></tr>
<tr><td>3</td><td colspan="3">IP</td></tr>
<tr><td>2</td><td colspan="5" rowspan="2">other</td></tr>
<tr><td>1</td></tr>
</table>

Data Transport: Differences IF-T and IF-WAN

- Most differences concern the use of TLS
- TCG specifications have a lot of recommendations for the use of TLS to make it flexible
- TCG recommendations regarding TLS are …
  - partially considered mandatory by the BSI
  - partially prohibited by the BSI
- At least one element specified by the TCG for TLS is fully contradicting:
  - Cipher suite TLS_RSA_WITH_AES_128_CBC_SHA

Data Transport: Custom IF-T



EVALUATION

Evaluation: Criteria

- Criteria based on ISO 25010 quality model:
  - Functionality
  - Complexity
  - Flexibility
  - Efficiency
  - Security
  - Standard orientation
- No approach was unsuitable at all

Evaluation: Approaches

- IF-T-BSI: Strong orientation on TCG specifications
- IF-T-BSI-EXT: Good efficiency and good functionality (best rating)
- IF-T-RS-COSEM: Very complex and BSI compliance not clear (worst rating)
- IF-T-RS-TNC: High flexibility and little to no standard orientation
- IF-T-RS-SIMPLE: Tradeoff between IF-T-BSI and IF-T-RS-TNC

Evaluation: Final Result

- DLMS/COSEM RESTful web service should be used to configure TNC at the SMGW
- IF-T-BSI should be used for the transmission of TNC data
  - Not the best rated approach but:
    - Strong orientation on TCG specifications
    - Less complex (TLS only)
    - Theoretically compatible to existing TNC implementations (low adoption barrier)
    - TCG specifications are more mature than the specifications of the BSI

CONCLUSION & PROSPECTS

Conclusion

- Demonstration of TNC for a Smart Metering System was implemented
  - Integration of an AR at an SMGW
  - Integration of a PDP at a GWA
  - Configuration of TNC at the SMGW can be done using the DLMS/COSEM RESTful web service
- Different approaches for the transmission of TNC-Data where introduced
  - The approach with the strongest orientation on the TCG specifications was chosen to lower the adoption barrier

Prospects

- The results of this paper have to be discussed further with the TCG
- Development of a Trusted Grid using TNC for other components in the Smart Grid
- Integration of further (TNC-)components for monitoring the Smart Metering System as well as the Smart Grid
- Open Source project for a Java based TNC library (jTNC): https://github.com/trusthsbremen/jtnc

Thank You

HSB
Hochschule Bremen
City University of Applied Sciences

Questions?