Smart home and building solutions.
Global. Secure. Connected.

Network Intrusion Detection in Building Automation Systems

Alija Sabic, FH Technikum Wien
Wolfgang Granzer, NETx Automation
Friedrich Praus, FH Technikum Wien

Outline

Unsecured BAS Installations (Worldwide, 2016)

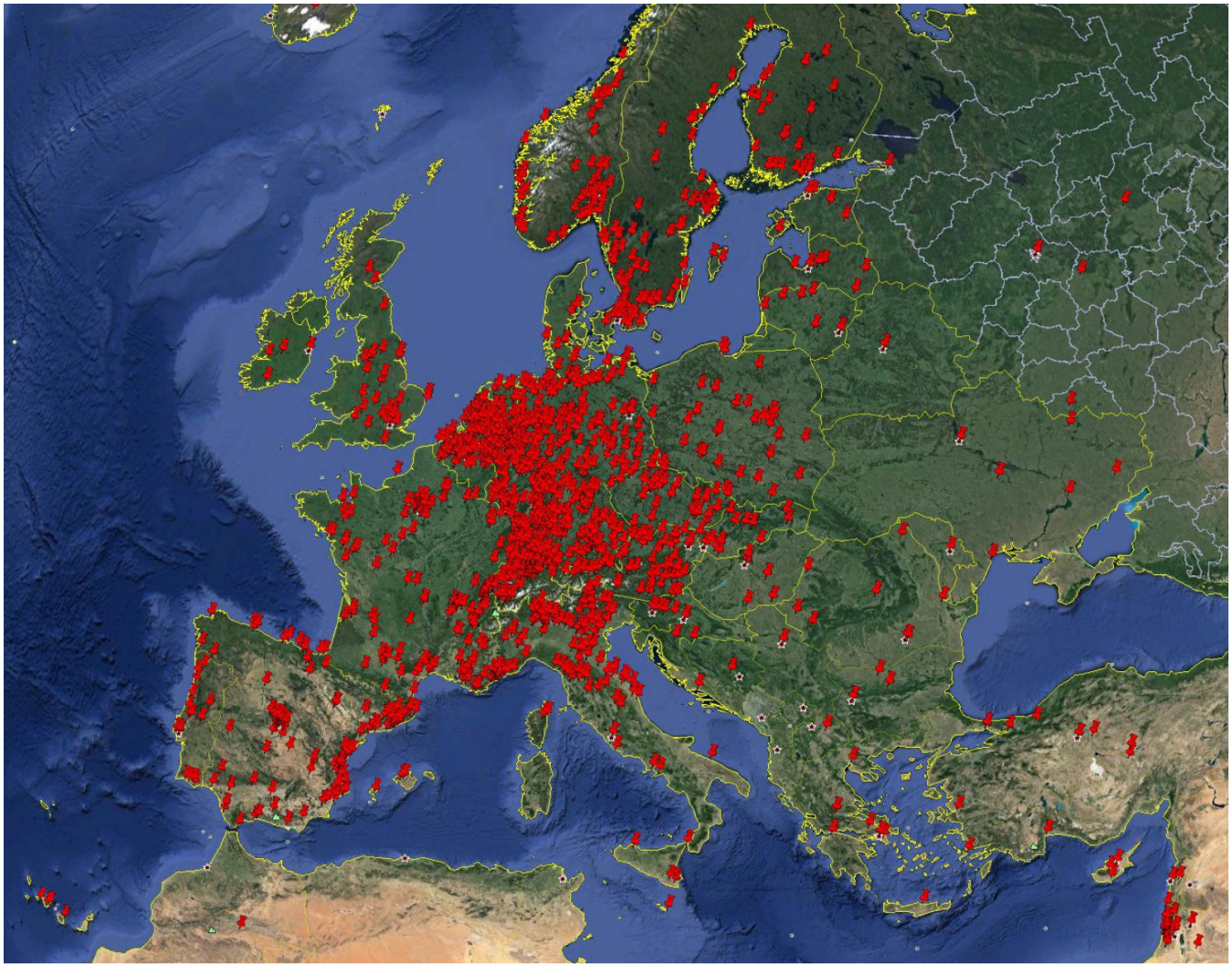

Figure 1: Unsecured Installations in Europe [1]

Unsecured BAS Installations (Worldwide, 2016)

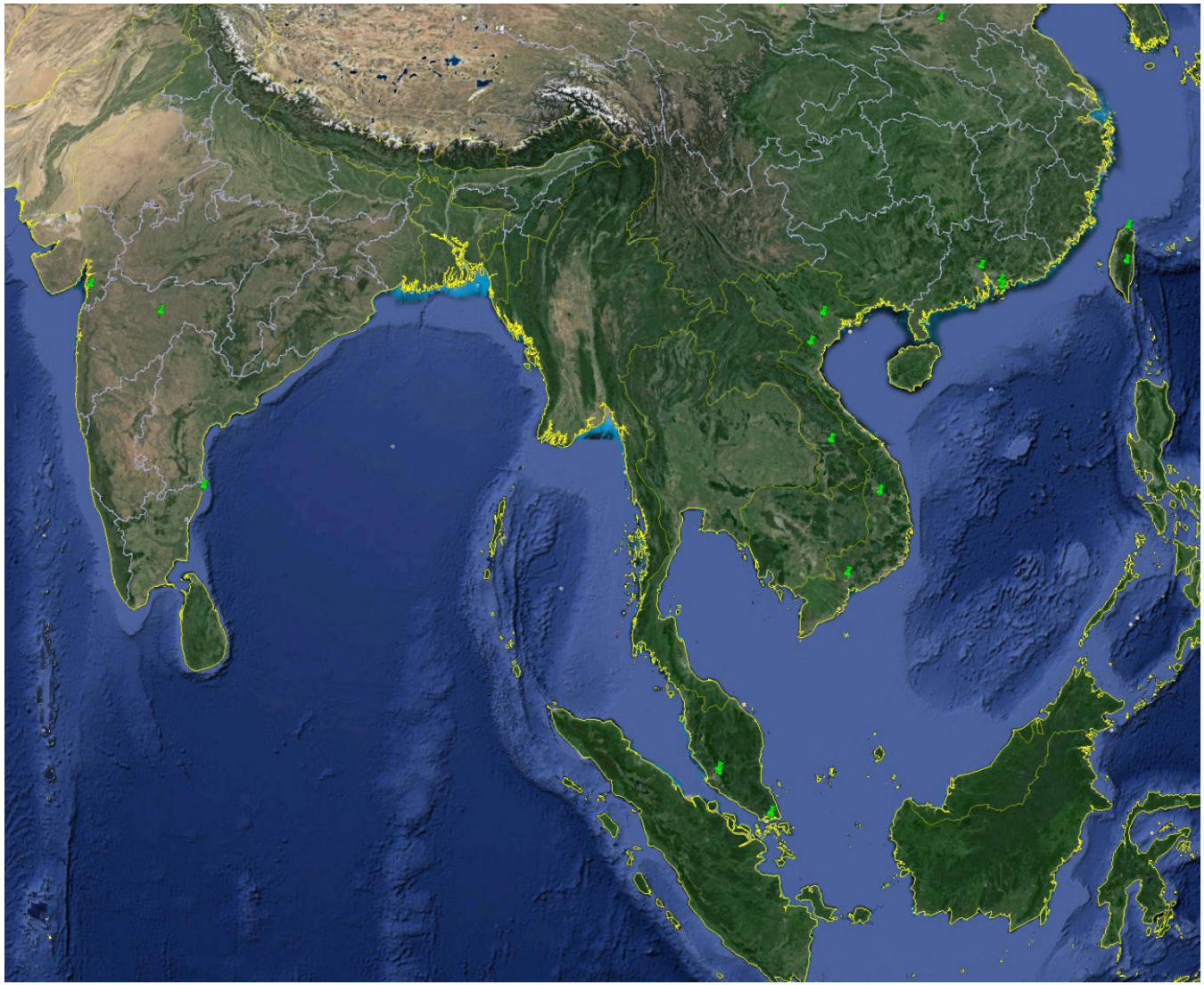

Figure 2: Unsecured Installations in Asia [1]

Unsecured BAS Installations (Worldwide, 2016)

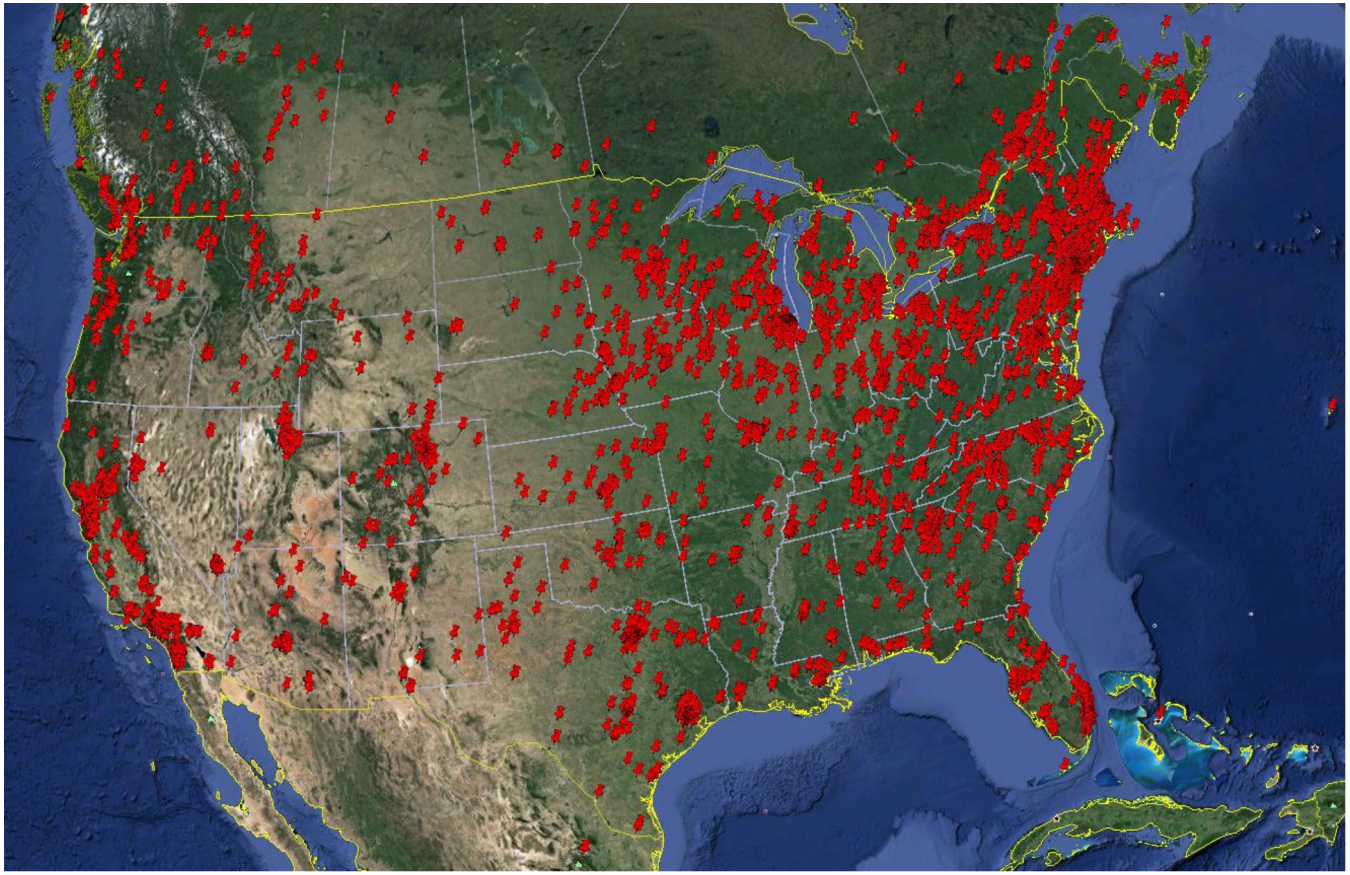

Figure 3: Unsecured Installations in North America [1]

Defense in Depth

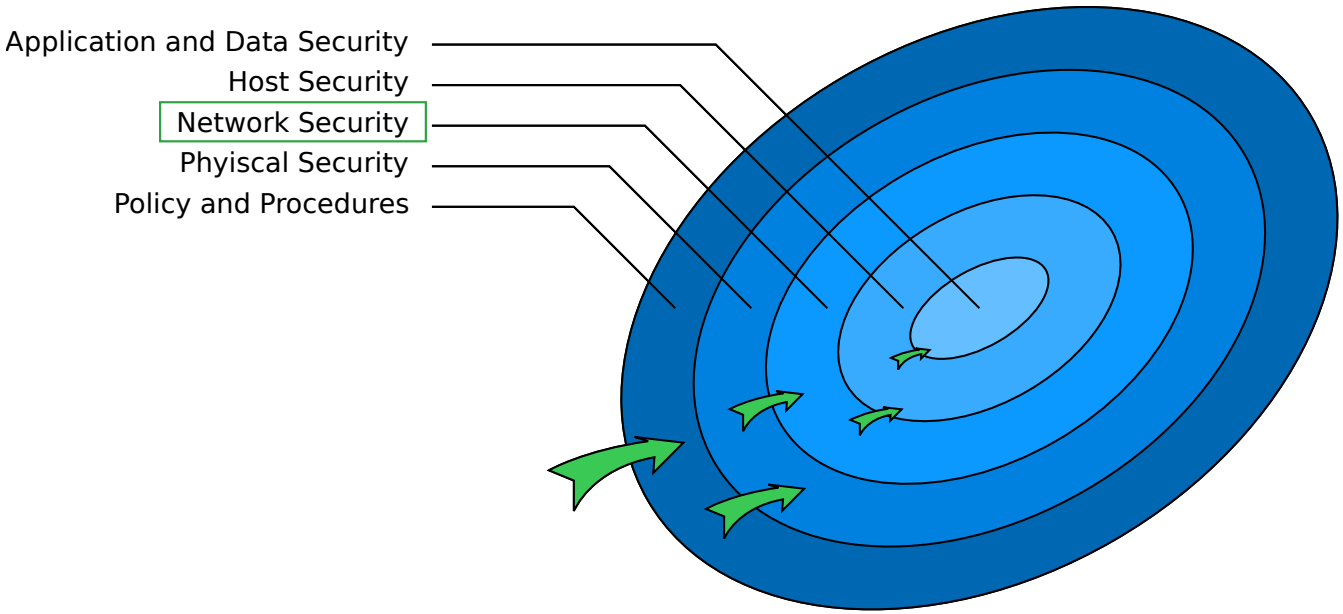

Figure 5: Layered Security [2][3]

Task Description

- Develop an IDS that can be used for BAS
- The IDS should support installations based on
  - KNX
  - BACnet
  - EnOcean
- The IDS should base on open-source software
- The IDS should be easy to handle by facility management and IT security personnel

Detection Methodologies

Signature-based Detection (SD)

SD is the process using signatures, i.e., patterns or strings, to compare patterns against captured events to recognize possible intrusions.

Anomaly-based Detection (AD)

AD is the process of comparing definitions of regular activity against observed events to identify significant deviations.

Stateful Protocol Analysis (SPA)

SPA is the process of comparing profiles of generally excepted protocol activity for each state against observed events. SPA is able to track and understand states of network, transport and application protocols.

Detection Approaches

	Detection approach	Detection methodology[a]			Time Series	Technology type[b]	Detection of attacks[c]	Performance[d]
		AD	SD	SPA				
Statistics-based	Statistics	✓	✓	–	O	H/N	B	M
	Distance-based	✓	–	–	O	N	U	M
	Bayesian-based	✓	✓	–	O	N	B	H
	Game Theory	✓	–	–	O	H/N	U	L
Pattern-based	Pattern Matching	–	✓	–	✗	N	K	H
	Petri Net	–	✓	–	O	H	K	M
	Keystroke monitoring	–	✓	–	O	H	K	H
	File system checking	✓	✓	–	✗	H	B	H
Rule-based	Rule-based	✓	✓	–	✗	H/N	B	H
	Data Mining	✓	✓	–	✗	N	B	M
	Model/Profile-based	✓	–	–	✗	H/N	U	M
	Support vector machine	✓	✓	–	O	N	B	H
State-based	State-Transition Analysis	–	✓	–	O	H/N	K	H
	User intention identification	✓	–	–	O	H	U	H
	Markov Process Model	✓	–	–	O	H/N	U	M
	Protocol Analysis	✓	✓	✓	O	P	T	L
Heuristic-based	Neural Networks	✓	✓	–	O	N	B	M
	Fuzzy Logic	✓	–	–	✗	H/N	U	H
	Genetic algorithm	–	✓	–	O	N	K	L
	Immune system	✓	✓	–	O	H	B	M
	Swarm Intelligent	✓	–	–	O	N	U	H

[a] Detection methodology: anomaly-based detection (AD), signature-based detection (SD), stateful protocol analysis (SPA).
[b] Technology type: host-based (H), network-based (N), protocol-based (P).
[c] Detection of attacks: known attacks (K), unknown attacks (U), both known and unknown attacks (B), tripartite of AD, SD, SPA (T).
[d] Performance: high (H), moderate (M), low (L).

Table 1: Classification of various intrusion detection approaches [4]

Snort 3.0

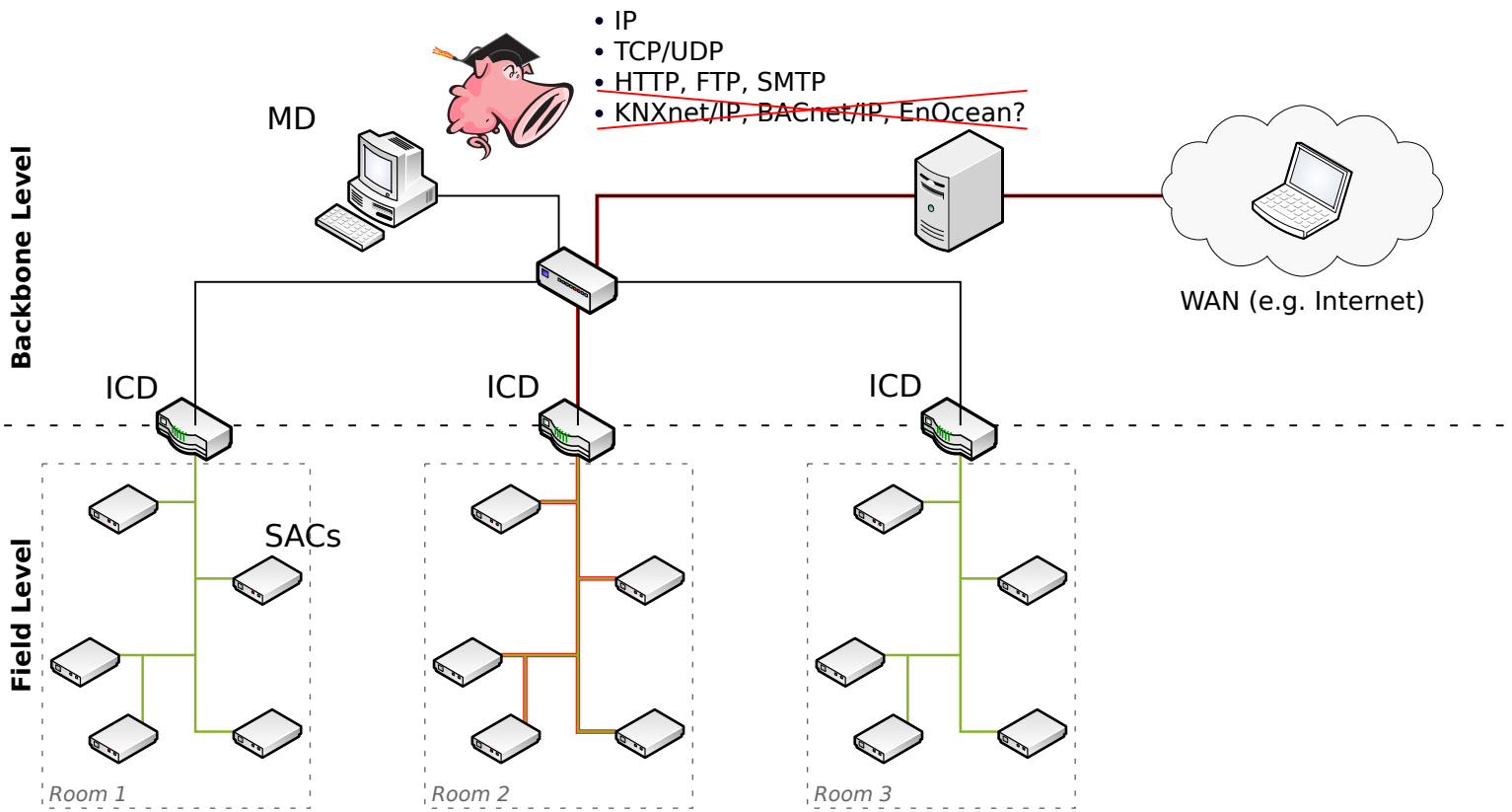

Figure 6: Snort 3.0

Snort 3.0 Architecture

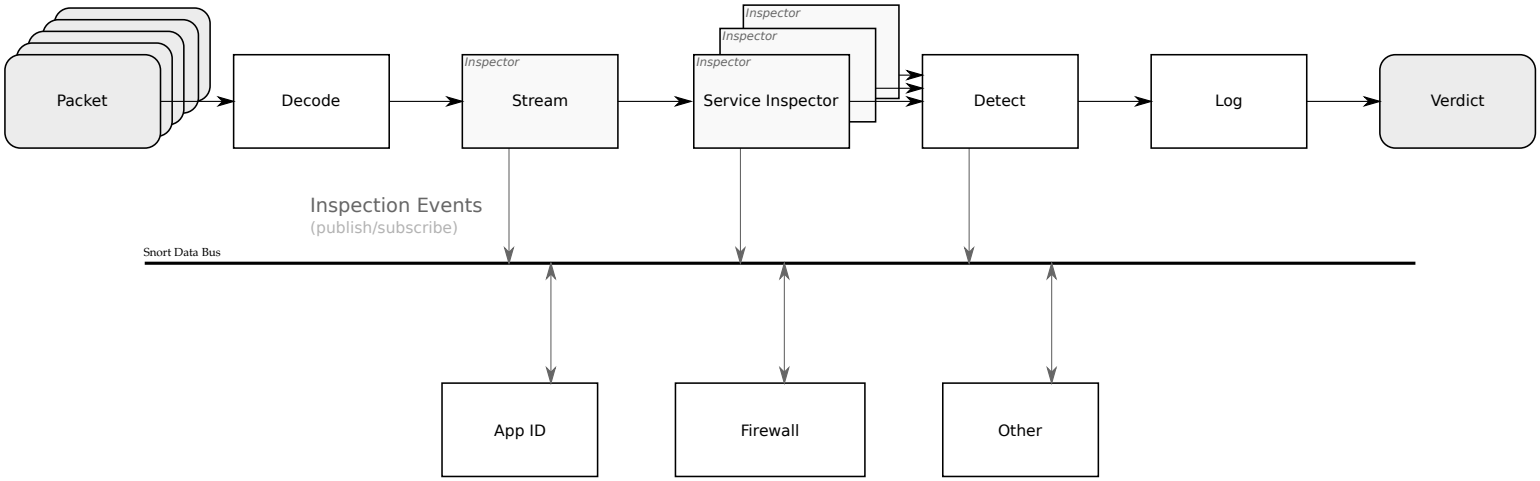

Figure 7: Snort 3.0 Architecture [5]

Rules

```
1 action proto source dir dest ( body )
```

Listing 1: Snort rule structure

```
1 log tcp any any -> 10.0.0.1/24 79 (msg:"TCP ↵
      traffic on host X at port Y.";)
```

Listing 2: Snort rule example

```
1 alert tcp any any -> 192.168.1.1 80 ( msg:"A ↵
      ha!"; content:"attack"; sid:1; )
```

Listing 3: Snort rule example (SD)

```
1 alert http (
2     msg:"Catch 'em all!";
3     flow:estabilished;
4     to_server;
5     http_uri:"attack";
6     sid:2;
7 )
```

Listing 4: Snort rule example (SPA)

KNXnet/IP Service Inspector

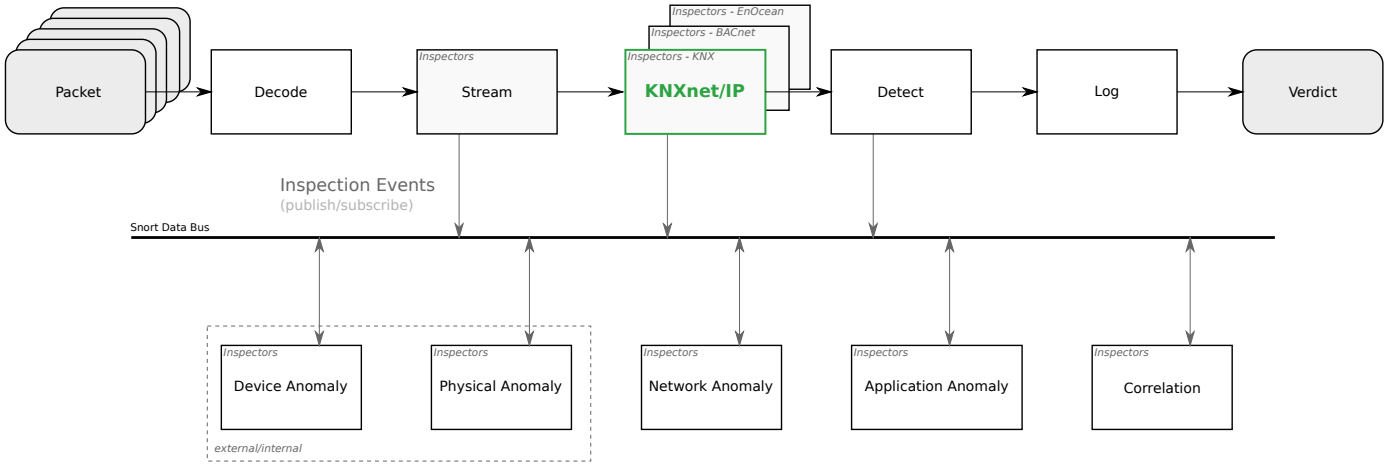

Figure 8: KNXnet/IP Service Inspector [6]

Execution Flow

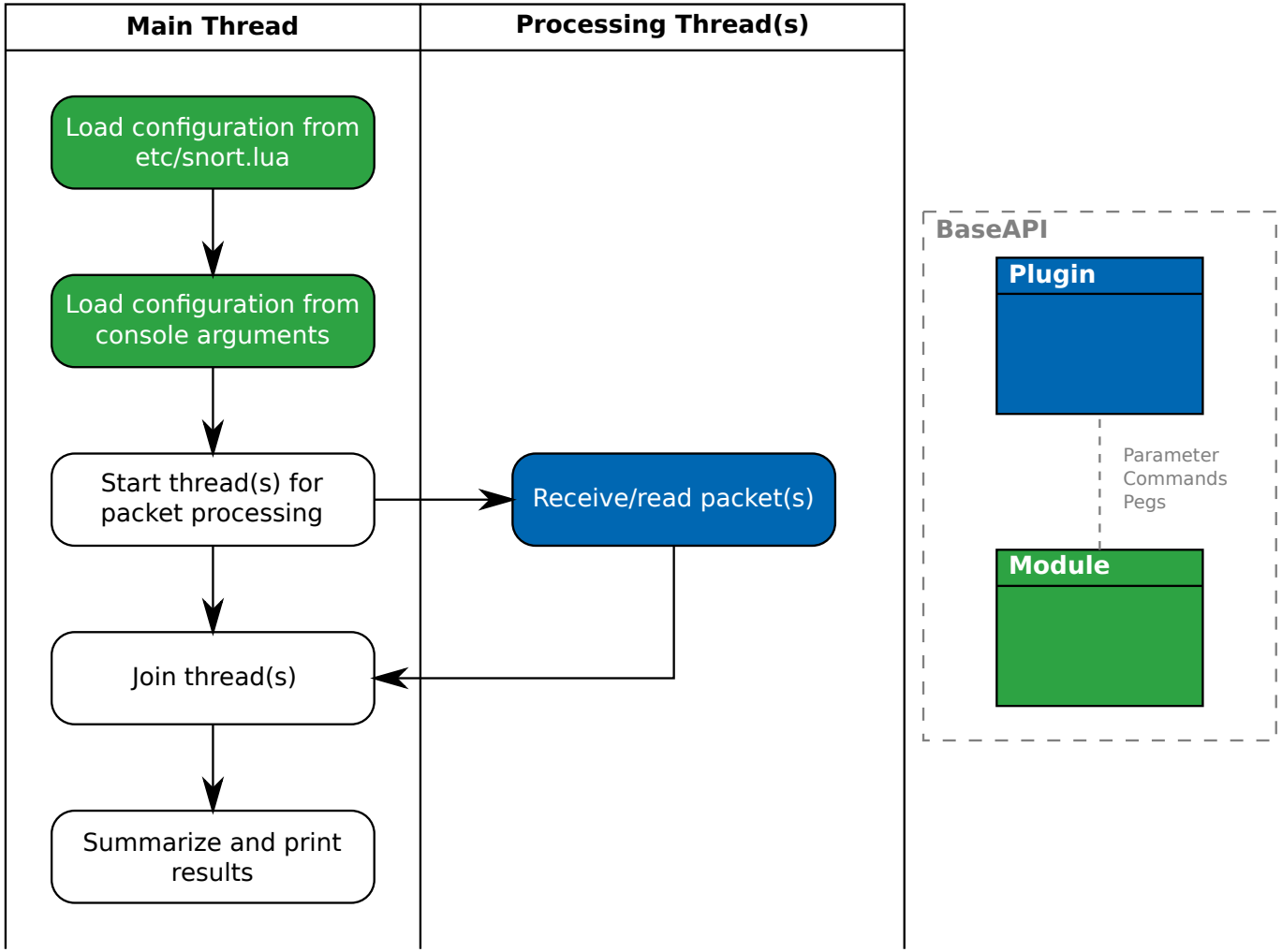

Figure 9: Snort's Execution Flow & Packet Processing

Configuration

- Two types of objects:
  - `server`
  - `policy`
- `server` object used to define:
  - IP, Port, and Policy
  - Logging
- `policy` object used to define:
  - Protocol Inspection
  - Anomaly Detection
    - Individual/Physical Addressing
    - KNXnet/IP Services
    - KNX Application Layer Services
    - Group Address File

ETS Group Address Export

```
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<GroupAddress-Export xmlns="http://knx.org/xml/ga-export/01">
<GroupAddress Name="Central" Address="0/0/1" Central="true" DPTs="DPST-1-1"/>
<GroupAddress Name="Date and Time" Address="0/1/0" DPTs="DPT-19" />
<GroupAddress Name="Light A1 - Switch" Address="1/0/0" DPTs="DPST-1-1"
              ia="7.6.7,7.6.5"/>
<GroupAddress Name="Light B1 - Switch" Address="1/1/0" DPTs="DPST-1-1" />
<GroupAddress Name="J1 - Up/Down" Address="2/0/0" DPTs="DPST-1-8" />
<GroupAddress Name="J1 - Stop/Slat" Address="2/0/1" DPTs="DPST-1-9" />
<GroupAddress Name="J2 - Up/Down" Address="2/1/0" DPTs="DPST-1-8" />
<GroupAddress Name="J2 - Stop/Slat" Address="2/1/1" DPTs="DPST-1-9" />
<GroupAddress Name="Room B - Current Temp." Address="3/1/0" DPTs="DPST-9-1"
              max="30.0" min="15.0" ia="7.6.4" />
</GroupAddress-Export>
```

Listing 5: ETS GA export

ETS Group Address Export

```
<GroupAddress-Export>
    <GroupAddress
        Name="Light A1 - Switch"
        Address="1/0/0"
        DPTs="DPST-1-1"
        ia="7.6.7,7.6.5"
    />
    <GroupAddress
        Name="Room B - Current Temperature"
        Address="3/1/0"
        DPTs="DPST-9-1"
        max="30.0"
        min="15.0"
        ia="7.6.4"
    />
</GroupAddress-Export>
```

Listing 6: ETS GA export

Packet Processing & Protocol Inspection

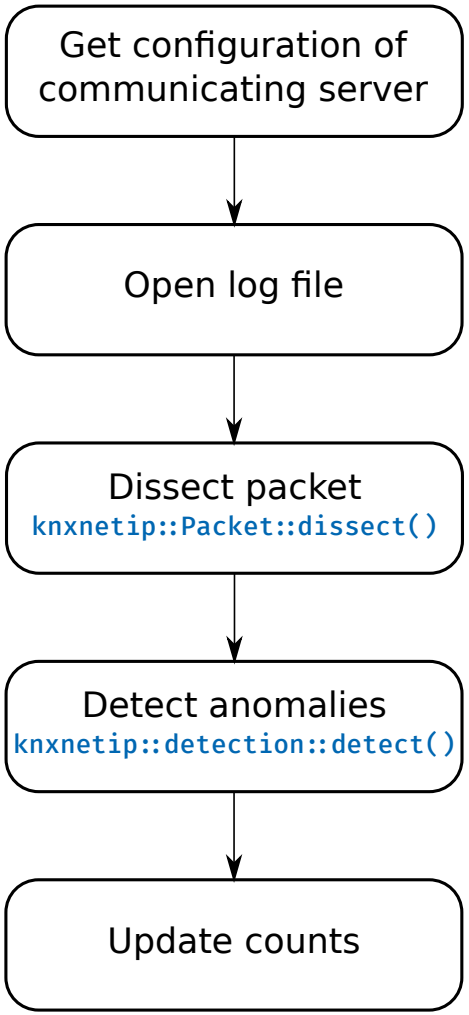

Figure 10: Inspector API: `eval()` routine

Anomaly Detection

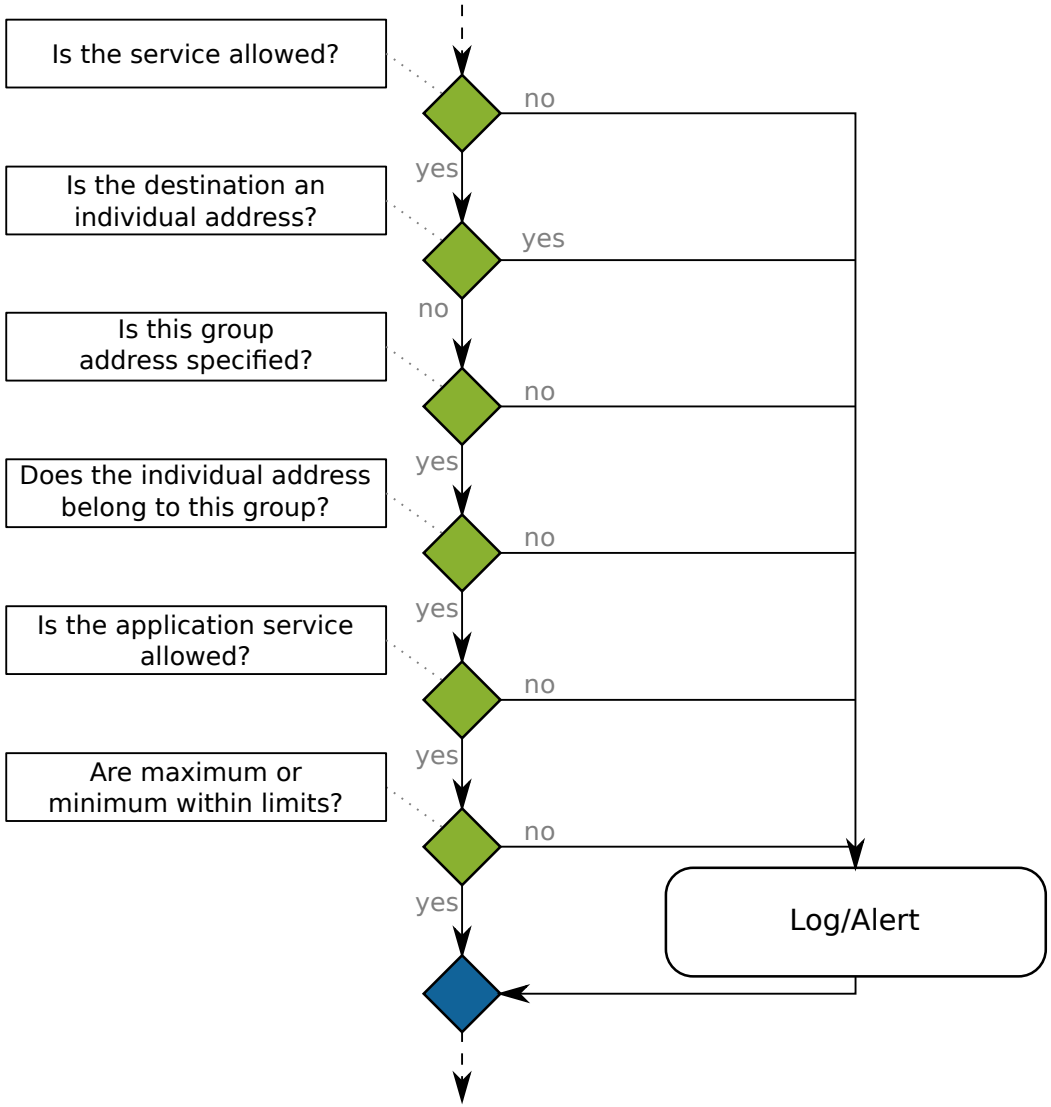

Figure 11: `knxnetip::detection::detect()`

Attack Scenario & Setup

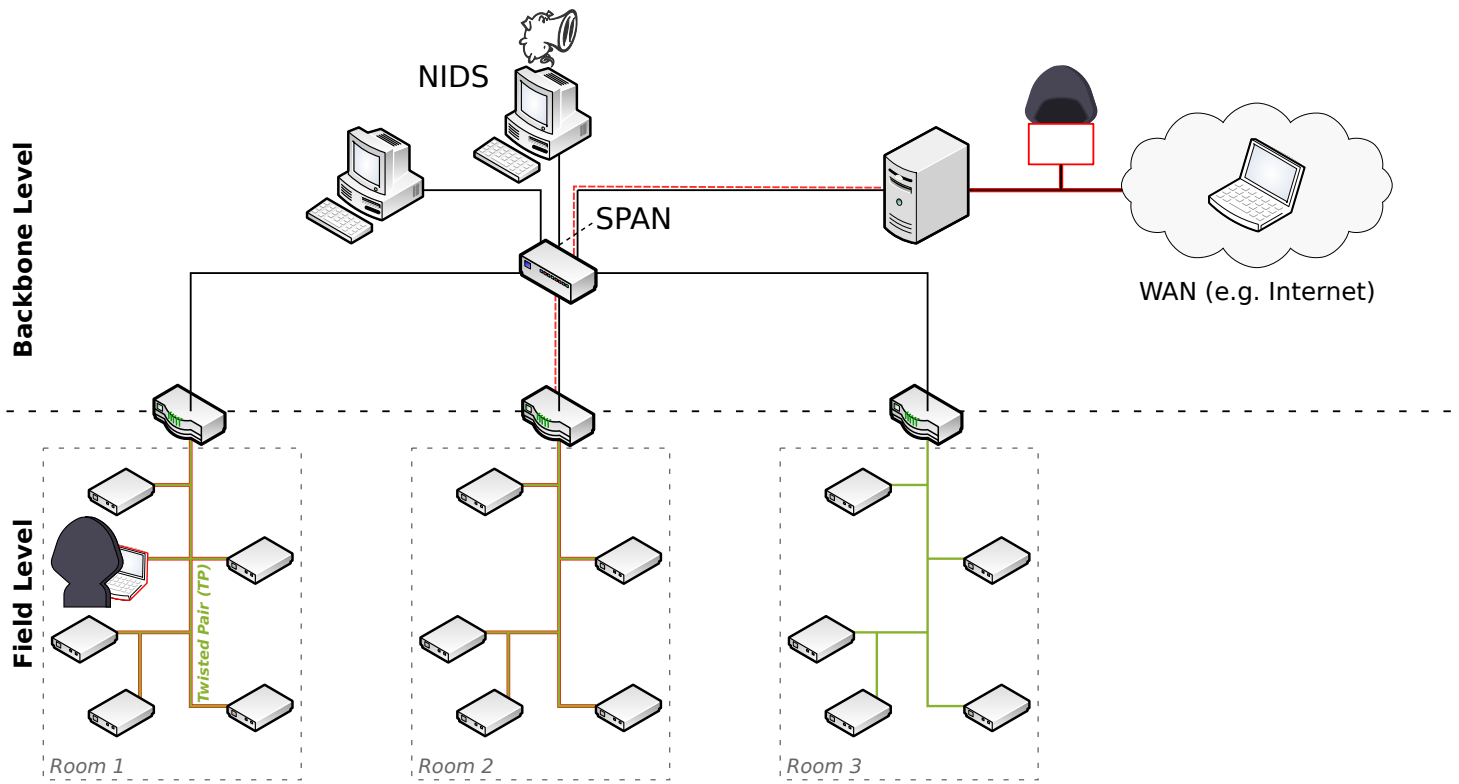

Figure 12: Attack Scenario

#1 Protocol Version

```
$ snort -c snort.lua -R local.rules -r INVALID_VERSION.pcap -A alert_full -d -X -e
```

```
++ [0] /home/admin/captures/INVALID_VERSION.pcap
pkt:1     gid:147    sid:3    rev:0
timestamp:08/22-14:27:08.000000
eth(DLT):  0A:01:01:01:01:01 -> 0A:02:02:02:02:02  type:0x0800
ipv4(0x0800):  172.22.10.76 -> 172.22.12.76
   Next:0x11 TTL:255 TOS:0x0 ID:4660 IpLen:20 DgmLen:51
udp(0x11):  SrcPort:3671 DstPort:41975 Len:23

knxnetip.raw[65]:
- -   - - - - - - - - - - - -  - - - - - - - - - - - -  - - - - - - - - -
0000  0A 02 02 02 02 02 0A 01  01 01 01 01 08 00 45 00  ........ ......E.
0010  00 33 12 34 00 00 FF 11  3A C1 AC 16 0A 4C AC 16  .3.4.... :....L..
0020  0C 4C 0E 57 A3 F7 00 1F  9A 51 06 20 04 20 00 17  .L.W.... .Q. . ..
0030  04 01 3E 00 29 00 BC E0  76 04 19 00 03 00 80 0D  ..>.)... v.......
0040  00                                               .
- -   - - - - - - - - - - - -  - - - - - - - - - - - -  - - - - - - - - -
[**] [147:2:0] "(knxnetip) invalid protocol version" [**]

-- [0] /home/admin/captures/INVALID_VERSION.pcap
```

Figure 13: Invalid protocol version alert

#2 Total Length

```
$ snort -c snort.lua -R local.rules -r INVALID_TOTAL_LENGTH.pcap -A alert_full -d -X -e
```

```
knxnetip.raw[65]:
- -   - - - - - - - - - - - -  - - - - - - - - - - - -  - - - - - - - -
0000  0A 02 02 02 02 02 0A 01  01 01 01 01 08 00 45 00  ........ ......E.
0010  00 33 12 34 00 00 FF 11  3A C1 AC 16 0A 4C AC 16  .3.4.... :....L..
0020  0C 4C 0E 57 A3 F7 00 1F  9A 60 06 10 04 20 00 18  .L.W.... .‘... .. 
0030  04 01 3E 00 29 00 BC E0  76 04 19 00 03 00 80 0D  ..>.)... v.......
0040  00                                               .
- -   - - - - - - - - - - - -  - - - - - - - - - - - -  - - - - - - - -
[**] [147:3:0] "(knxnetip) total length of packet does not match received length" [**]

-- [0] /home/admin/captures/INVALID_TOTAL_LENGTH.pcap
```

Figure 14: Invalid total packet length alert

#3 Covert Channels

```
$ snort -c snort.lua -R local.rules -r COVERT_CHANNEL.pcap -A alert_full -d -X -e
```

```
knxnetip.raw[60]:
- -   - - - - - - - - - - - -  - - - - - - - - - - - -  - - - - - - - -
0000  00 0E 8C 00 24 C3 28 D2  44 2C 68 DF 08 00 45 00  ....$.(. D,h...E.
0010  00 2C EC FE 40 00 40 11  46 72 A9 FE 59 A9 A9 FE  .,..@.@. Fr..Y...
0020  59 AA A0 A6 0E 57 00 18  68 2E 06 10 02 07 00 10  Y....W.. h.......
0030  41 FE 08 01 A9 FE 59 A9  8B 73 00 00              A.....Y. .s..
- -   - - - - - - - - - - - -  - - - - - - - - - - - -  - - - - - - - -
[**] [147:11:0] "(knxnetip) reserved protocol field with data" [**]

-- [0] /home/admin/captures/COVERT_CHANNEL.pcap
```

Figure 15: Non-null data in reserved protocol field

#4 Individual Adressing

```
$ snort -c snort.lua -R local.rules -r INDIVIDUAL_ADDRESSING.pcap -A alert_full -d -X -e
```

```
knxnetip.raw[65]:
- -   - - - - - - - - - - - - -  - - - - - - - - - - - - -  - - - - - - - - -
0000  0A 02 02 02 02 02 0A 01  01 01 01 01 08 00 45 00  ........ ......E.
0010  00 33 12 34 00 00 FF 11  3A C1 AC 16 0A 4C AC 16  .3.4.... :....L..
0020  0C 4C 0E 57 A3 F7 00 1F  41 C8 06 10 04 20 00 17  .L.W.... A.... ..
0030  04 17 B7 00 29 00 BC 60  76 04 76 03 03 00 80 0C  ....)..‘ v.v.....
0040  83                                               .
- -   - - - - - - - - - - - -  - - - - - - - - - - - - -  - - - - - - - - -
[**] [147:11:0] "(knxnetip) individual addressing: (7.6.3)" [**]

-- [0] /home/admin/captures/INDIVIDUAL_ADDRESS.pcap
```

Figure 16: Individual destination address alert

#5 Device Programming

```
$ snort -c snort.lua -R local.rules -r APP_SERVICES.pcap -A alert_full -d -X -e
```

```
knxnetip.raw[65]:
- -   - - - - - - - - - - - -  - - - - - - - - - - - -  - - - - - - - - -
0000  00 23 24 51 C3 D3 00 24  6D 00 C7 55 08 00 45 00  .#Q... m..U..E.
0010  00 33 70 65 00 00 10 11  C9 7C AC 16 0A 4C AC 16  .3pe.... .|...L..
0020  0E 60 0E 57 D1 F5 00 1F  0B D1 06 10 04 20 00 17  .‘.W.... ..... ..
0030  04 15 74 00 29 00 B0 E0  76 05 00 00 03 00 C0 76  ..t.)... v......v
0040  0D                                               .
- -   - - - - - - - - - - - -  - - - - - - - - - - - -  - - - - - - - - -
[**] [147:14:0] "(knxnetip) illegal application layer service type: ↵
       A_IndividualAddress_Write" [**]

-- [0] /home/admin/captures/APP_SERVICES.pcap
```

Figure 17: application layer service alert

#6 Group Address

```
$ snort -c snort.lua -R local.rules -r GROUP_ADDRESS.pcap -A alert_full -d -X -e
```

```
knxnetip.raw[65]:
- -   - - - - - - - - - - - -  - - - - - - - - - - - -  - - - - - - - - -
0000  0A 02 02 02 02 02 0A 01  01 01 01 01 08 00 45 00  ........ ......E.
0010  00 33 12 34 00 00 FF 11  3A C1 AC 16 0A 4C AC 16  .3.4.... :....L..
0020  0C 4C 0E 57 A3 F7 00 1F  97 4A 06 10 04 20 00 17  .L.W.... .J... ..
0030  04 17 B7 00 29 00 BC E0  76 04 20 01 03 00 80 0C  ....)... v. .....
0040  83                                               .
- -   - - - - - - - - - - - -  - - - - - - - - - - - -  - - - - - - - - -
[**] [147:12:0] "(knxnetip) illegal group address: (4/0/1) or (4/1)" [**]

-- [0] /home/admin/captures/GROUP_ADDRESS.pcap
```

Figure 18: Invalid group address alert

#7 Maxima, Minima

```
$ snort -c snort.lua -R local.rules -r EXTREMA.pcap -A alert_full -d -X -e
```

```
knxnetip.raw[65]:
- -   - - - - - - - - - - - -  - - - - - - - - - - - -  - - - - - - - -
0000  0A 02 02 02 02 02 0A 01  01 01 01 01 08 00 45 00  ........ ......E.
0010  00 33 12 34 00 00 FF 11  3A C1 AC 16 0A 4C AC 16  .3.4.... :....L..
0020  0C 4C 0E 57 A3 F7 00 1F  B6 59 06 10 04 20 00 17  .L.W.... .Y... ..
0030  04 07 A1 00 29 00 BC E0  76 04 19 00 03 00 80 0E  ....)... v.......
0040  81                                               .
- -   - - - - - - - - - - - -  - - - - - - - - - - - -  - - - - - - - -
[**] [147:19:0] "(knxnetip) value out of range (max): 33.3 °C (Maximum: 32.75 °C)" [**]

-- [0] /home/admin/captures/EXTREMA.pcap
```

Figure 19: Maxima alert

#7 Maxima, Minima

```
$ snort -c snort.lua -R local.rules -r EXTREMA.pcap -A alert_full -d -X -e
```

```
knxnetip.raw[65]:
- -   - - - - - - - - - - - -  - - - - - - - - - - - -  - - - - - - - - -
0000  0A 02 02 02 02 02 0A 01  01 01 01 01 08 00 45 00  ........ ......E.
0010  00 33 12 34 00 00 FF 11  3A C1 AC 16 0A 4C AC 16  .3.4.... :....L..
0020  0C 4C 0E 57 A3 F7 00 1F  0C 5E 06 10 04 20 00 17  .L.W.... .^... ..
0030  04 07 A1 00 29 00 BC E0  76 04 19 00 03 00 80 0A  ....)... v.......
0040  2B                                               +
- -   - - - - - - - - - - - -  - - - - - - - - - - - -  - - - - - - - - -
[**] [147:20:0] "(knxnetip) value out of range (min): 11.1 °C (Minimum: 12.50 °C)" [**]

-- [0] /home/admin/captures/EXTREMA.pcap
```

Figure 20: Minima alert

#8 Group Members

```
$ snort -c snort.lua -R local.rules -r GROUP_MEMBERS.pcap -A alert_full -d -X -e
```

```
knxnetip.raw[63]:
- -   - - - - - - - - - - - -  - - - - - - - - - - - -  - - - - - - - - -
0000  B8 27 EB 3C 91 42 00 24  6D 00 C7 55 08 00 45 00  .'.<.B.$ m..U..E.
0010  00 31 F0 3F 00 00 10 11  4B B8 AC 16 0A 4C AC 16  .1.?.... K....L..
0020  0C 4C 0E 57 A1 CD 00 1D  6C D2 06 10 04 20 00 15  .L.W.... l.... ..
0030  04 06 A5 00 2E 00 BC E0  53 CA 00 01 01 00 81     ........ S......
- -   - - - - - - - - - - - -  - - - - - - - - - - - -  - - - - - - - - -
[**] [147:18:0] "(knxnetip) illegal individual address 5.3.202 (Central, group: 0/0/1
       or 0/1, members: 7.6.2,7.6.4,7.6.7)" [**]

-- [0] /home/admin/captures/GROUP_MEMBERS.pcap
```

Figure 21: Individual Address is not a group member

Outlook

- Bridge semantic gap between IDS and BAS
- PCAP dumps of real-life BAS deployments [7]
- Freely available, readily accessible specification

Acronyms

AD	Anomaly-based Detection
AL	Application Layer
BACnet	Building Automation and Control Networks
BAS	Building Automation System
GA	Group Address
IDS	Intrusion Detection System
IP	Internet Protocol
IT	Information Technology
KNX	Konnex
PCAP	Packet Capture
SD	Signature-based Detection
SPA	Stateful Protocol Analysis

References I

[1] F. Praus, "Secure Control Applications in Smart Homes and Buildings," Ph.D. dissertation, Vienna University of Technology, 2015.

[2] J. D. Wilamowski, Bogdan M.; Irwin, *Industrial Communication Systems*. CRC Press, 2011.

[3] NCCIC and ICS-CERT, "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies Industrial Control Systems Cyber Emergency Response Team," Tech. Rep., 2016. [Online]. Available: https://goo.gl/32SFfe

[4] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 16–24, 2013. [Online]. Available: https://doi.org/10.1016/j.jnca.2012.09.004

References II

[5] The Snort Project, "Snort 3 User Manual," Tech. Rep., 2017. [Online]. Available: https://goo.gl/6kKcp2

[6] Alija Sabic, "Snort 3: KNXnet/IP Service Inspector," 2018. [Online]. Available: https://github.com/sabicalija/snort3/tree/master_thesis

[7] ——, "BAS Packet Captures (BACnet, KNX, EnOcean)," 2018. [Online]. Available: https://github.com/sabicalija/bas_pcap

[8] "KNX System Specification, Version 2.1, Konnex Association, ISO/IEC 14543-3," Jan 2014.

Appendix - BAS IDSs: A Structuring Appraoch

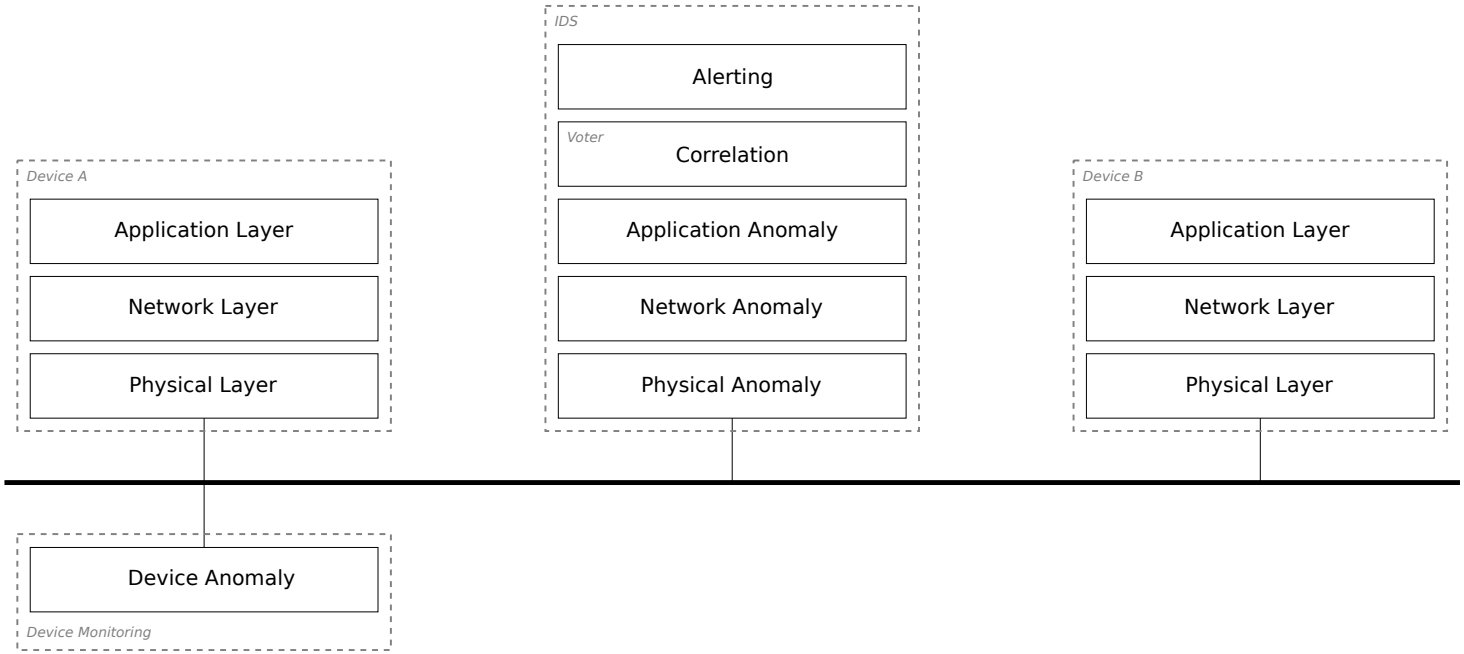

Figure 22: Generic Intrusion Detection System Architecture for BAS

Appendix - Detection Capabilities

```
$ snort -help-module knxnetip
```

knxnetip

Rules:

```
147:1 (knxnetip) erroneous packet content
147:2 (knxnetip) invalid header size
147:3 (knxnetip) invalid protocol version
147:4 (knxnetip) total length of packet does not match received length
147:5 (knxnetip) invalid service type
147:6 (knxnetip) total length of packet does not match expected length
147:7 (knxnetip) unsupported DIB type
147:8 (knxnetip) unsupported connection type
147:9 (knxnetip) unsupported SELECTOR type
147:10 (knxnetip) unsupported application layer service type
147:11 (knxnetip) reserved protocol field with data
147:12 (knxnetip) unsupported CEMI service
147:13 (knxnetip) CEMI processing error
147:14 (knxnetip) individual addressing
147:15 (knxnetip) illegal service type
147:16 (knxnetip) illegal application layer service type
147:17 (knxnetip) illegal group address
147:18 (knxnetip) illegal individual address
147:19 (knxnetip) value out of range (max)
```

Figure 23: KNXnet/IP: help instructions, builtin rules

Appendix - Configuration File

```
1   ------------------------------------------------------------------------
2   -- Snort++ configuration
3   ------------------------------------------------------------------------
33  ------------------------------------------------------------------------
34  -- 3. configure inspection
35  ------------------------------------------------------------------------
40
41  knxnetip =
42  {
43      global_policy = 2,
44      policies =
45      {
46          {
47              inspection = true,
48              detection = true,
49              individual_addressing = true,
50              services = { 'SEARCH_REQUEST', 'DESCRIPTION_REQUEST' },
51              app_services = {
52                  'A_IndividualAddress_Write',
53                  'A_IndividualAddress_Read'
54              },
55              group_address_level = 3,
56              group_address_file = 'etc/knxnetip/group_address.xml',
57              header = true,
58              payload = true
59          },
60          {
61              detection = true,
62              individual_addressing = true
63          }
64      },
65      servers =
66      {
67          { .. },
68          { .. }
69      }
70  }
71
72  ------------------------------------------------------------------------
```

Listing 7: KNXnet/IP Service Inspector Configuration Example

Appendix - ETS Group Address Export

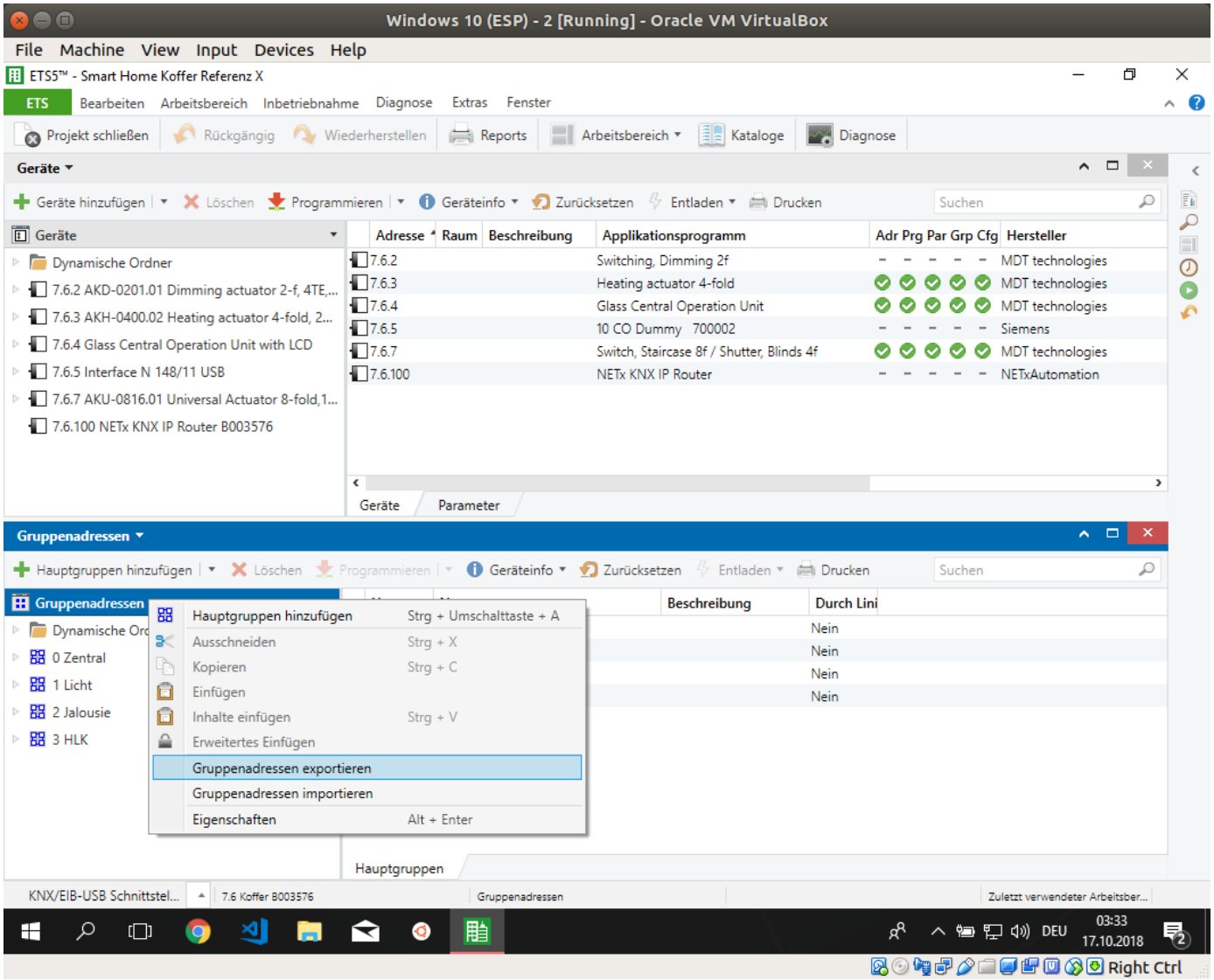

Figure 24: ETS Group Address Export (1/2)

Appendix - ETS Group Address Export

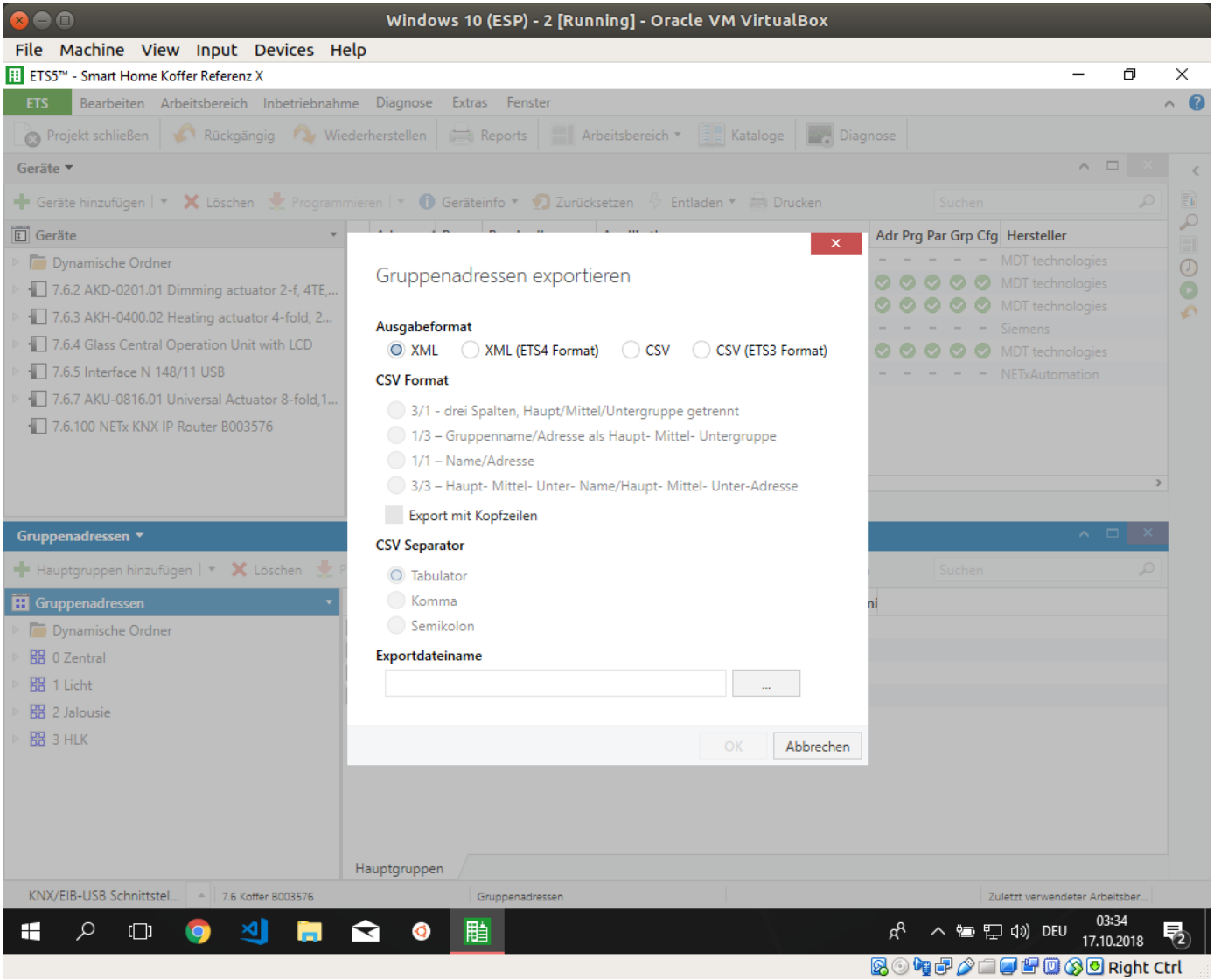

Figure 25: ETS Group Address Export (2/2)

Appendix - KNXnet/IP Protocol

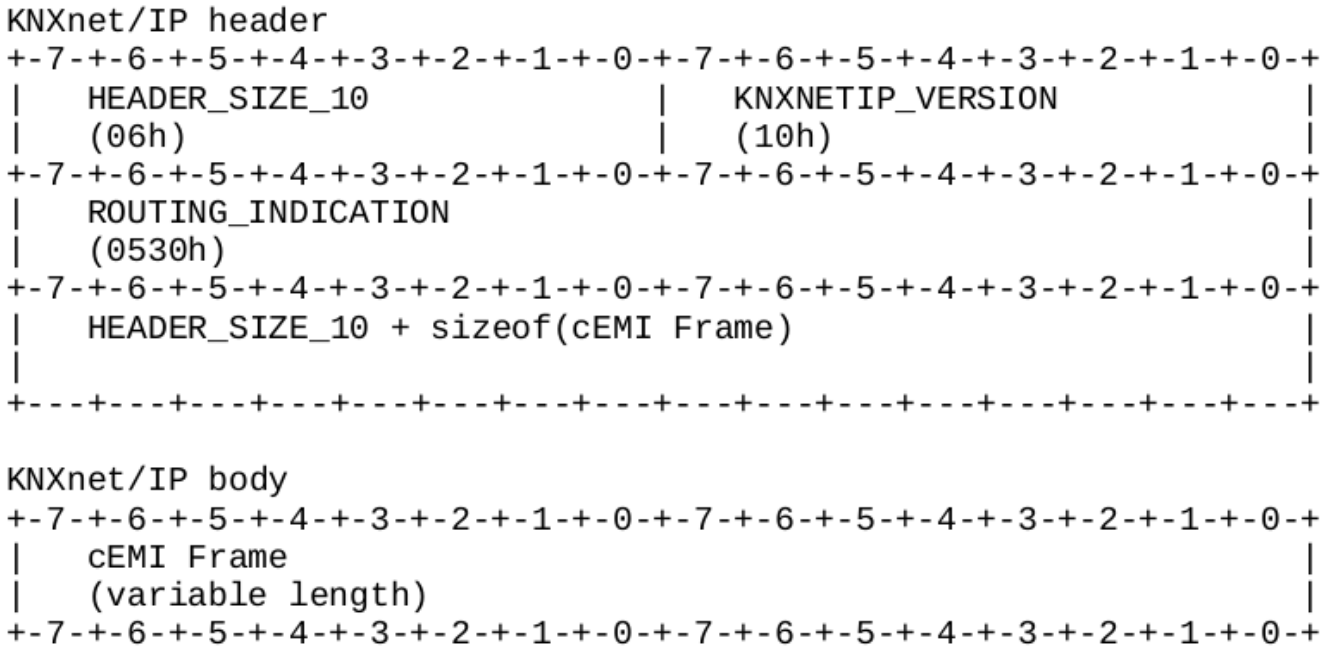

Figure 26: KNXnet/IP Protocol: Header & Body [8]

Appendix - KNXnet/IP Body, L_Data Service

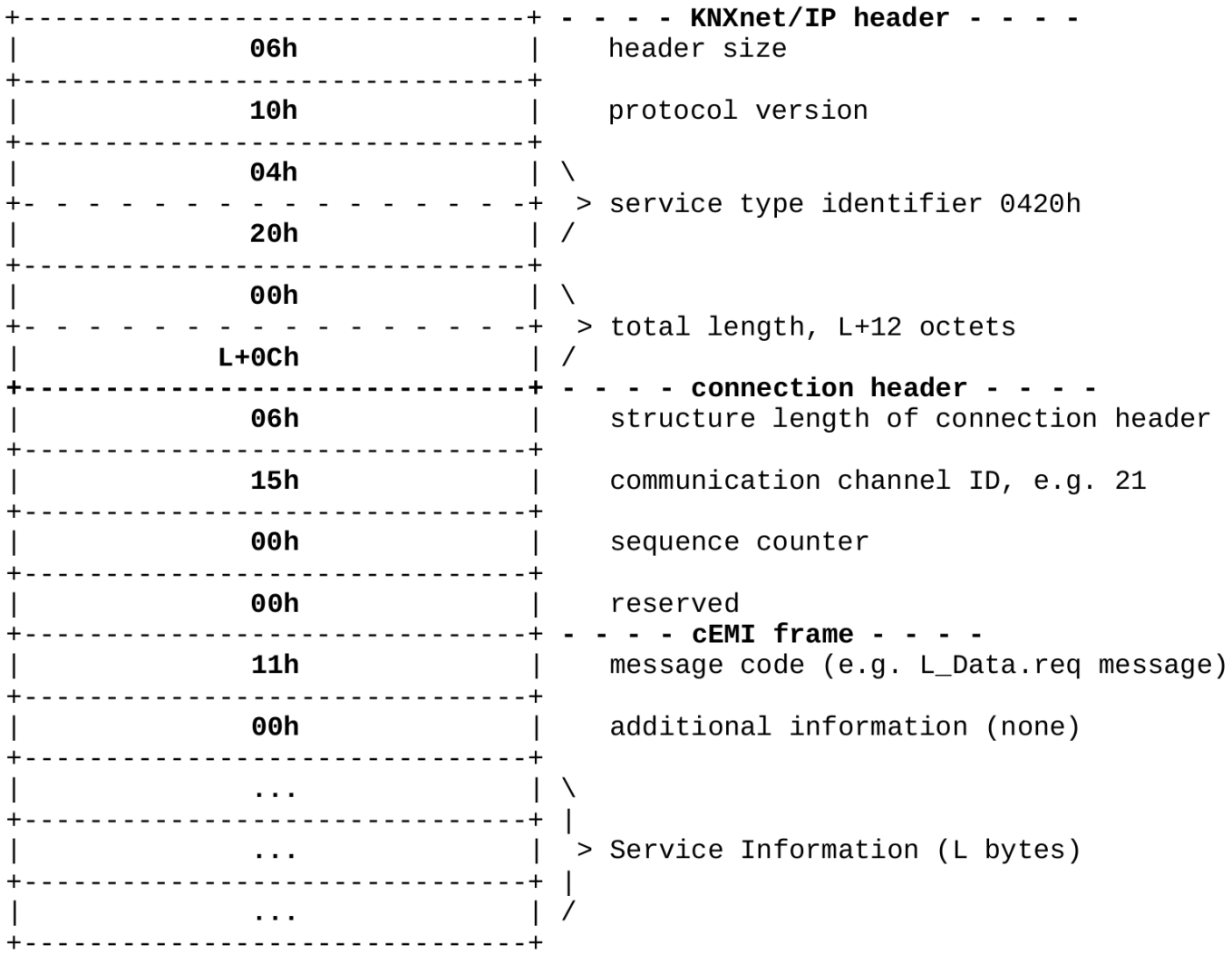

Figure 27: KNXnet/IP TUNNELLING_REQUEST [8]

Appendix - L_Data Service Frame Structure

Message Code	Additional Info Length	Additional Information	Control field 1	Control field 2	Src. High	Src. Low	Dest. High	Dest. Low	NPDU	
MC	**AddIL**	**…**	**Ctrl1**	**Ctrl2**	**SAH**	**SAL**	**DAH**	**DAL**	**L**	TPCI/APCI & data
1 octet	1 octet	var. length	1 octet	1 octet	2 octets		2 octets		1 octet	var. length

Figure 28: L_Data Service Frame Structure (cEMI) [8]

Ctrl2: Control field 2

1 octet							
Ctrl2							
7	6	5	4	3	2	1	0
AT	HC			EFF			

- Destination Address Type(AT) (msb):
  encoding: 0: individual
  1: group
- Hop Count (HC) (bit 6 to bit 4):
  encoding: value binary encoded
- Extended Frame Format (EFF) (bit 3 to bit 0 (lsb)):
  encoding: 0000b: for standard frame (long frames, APDU > 15 octet)
  01xxb: for LTE frames

Figure 29: Control Field 2 [8]