Conférence francophone d'informatique en Parallélisme, Architecture et Système

Contribution à l'adoption des IDS dans l'IoT

Cas d'un contexte grand public de type « smart home »

- **Olivier LOURME** olivier.lourme@univ-lille.fr
  - Part time PhD candidate
  - Part time Electrical Engineering teacher - Université de Lille (F)

- **CRIStAL Laboratory** (UMR 9189 - CNRS / Université de Lille)
  - 2XS (*eXtra Small eXtra Safe*) team led by Full Professor Gilles GRIMAUD
  - PhD supervised by Associate Professor Michaël HAUSPIE

Agenda

1 - IoT nodes are first choice targets for attackers

- IoT insights
- IoT inherent weaknesses
- Focus on smart-home ecosystem / Attacks examples

2 - IDS in a nutshell

- Introducing IDS
- Elements of IDS taxonomy
- A few IDS examples

3 - Characteristics of a smart home IDS

- Requirements of a smart-home protection x IDS taxonomy
- Proposed architecture

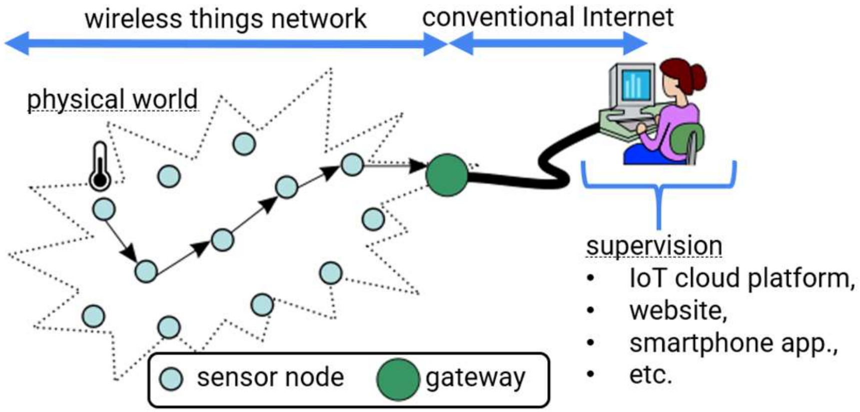
Conclusion, References

1 - IoT and security > IoT insights

What is “*Internet of Things*”? (ENISA, 2017) (Raza et al., 2013)

“ things”, “devices”, “nodes”, “hosts” or “objects” are:

- bridges between physical world and virtual world of supervision,
- communicating microcontrollers, with sensors or actuators,
- organized in wireless networks, often connected to the Internet.



WSN.svg: Public domain, via Wikimedia Commons

IoT:

- pervades all sci-tech fields,
- fosters fast decision making,
- has for 2025 estimation: (Lueth, 2018)
  - 21.5 billions things,
  - $1500 billions sales.

Credit : Internet of Things with Microcontrollers: a hands-on course - INRIA

1 - IoT and security> weaknesses / case of “smart-home” ecosystem

Weaknesses regarding IoT security:

- nodes low resources: ~~RSA~~,
- heterogeneities (µC / FreeRTOS, RIOT, Contiki, etc. / BLE, Zigbee, Wifi, 6LoWPAN, etc.),
- wireless comm. → eavesdropping, message injections, jamming.

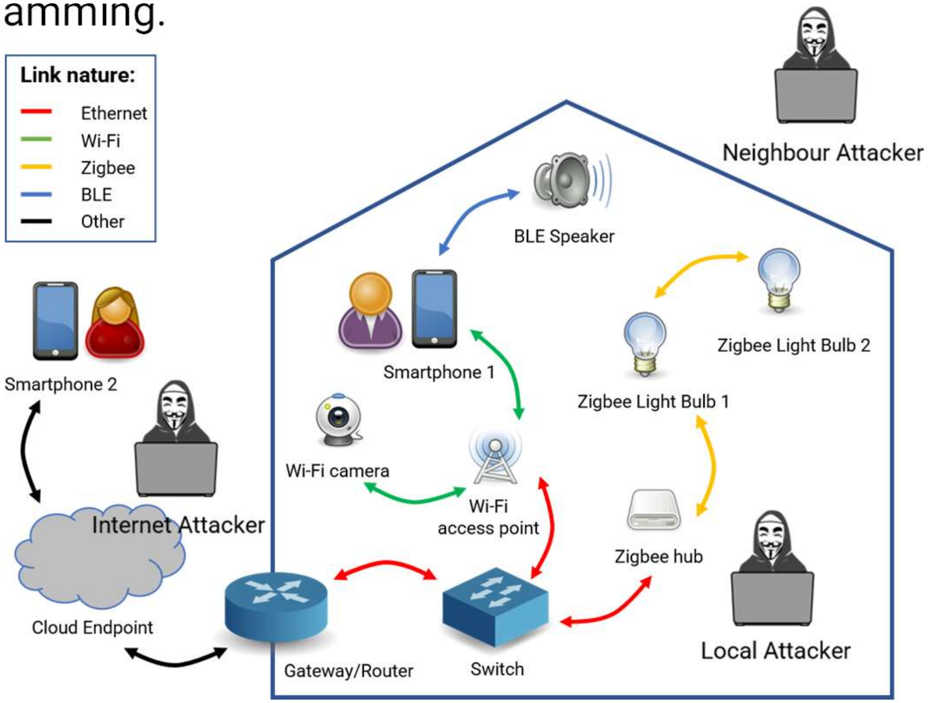
“Smart-home” ecosystem peculiarities:

- several protocol stacks under a small volume,
- a cost-driven market introducing many biases,
- non-technician users.

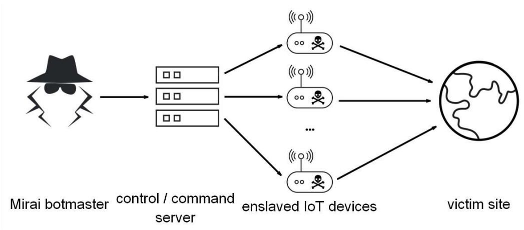
Requirements of a smart-home protection solution:

- coverage of most popular technologies and new ones,
- adapted cost (<100 €),
- standalone in already deployed sites, simple for users.

Threat model (Alrawi et al., 2019)



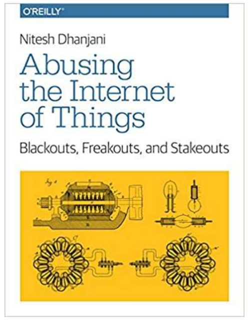
1 - IoT and security > examples of smart-home attacks



2016 – DDoS (Mirai malware)
Webcams default credentials
TCP/IP
(Kolias et al., 2017)

2018 – Door lock takeover
Insecure keys exchange
Z-Wave
(Khandelwal, 2018)

2016 – Confidentiality compromission
TC link key on forums → Network key
Zigbee
(Zillner, 2016)



O'REILLY

Nitesh Dhanjani

Abusing the Internet of Things

Blackouts, Freakouts, and Stakeouts

Attack use cases:
(Dhanjani, 2015)

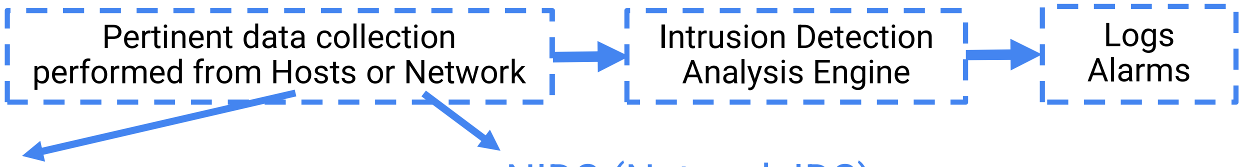
Attack taxonomy:
(Tschofenig and Baccelli, 2019)

There is a need for a first line of defense: Intrusion Detection Systems (IDS)

This presentation: Guidelines for a realistic smart-home IDS, widely adopted

2 - IDS in a nutshell > presentation and taxonomy

An IDS:



Pertinent data collection performed from Hosts or Network

Intrusion Detection Analysis Engine

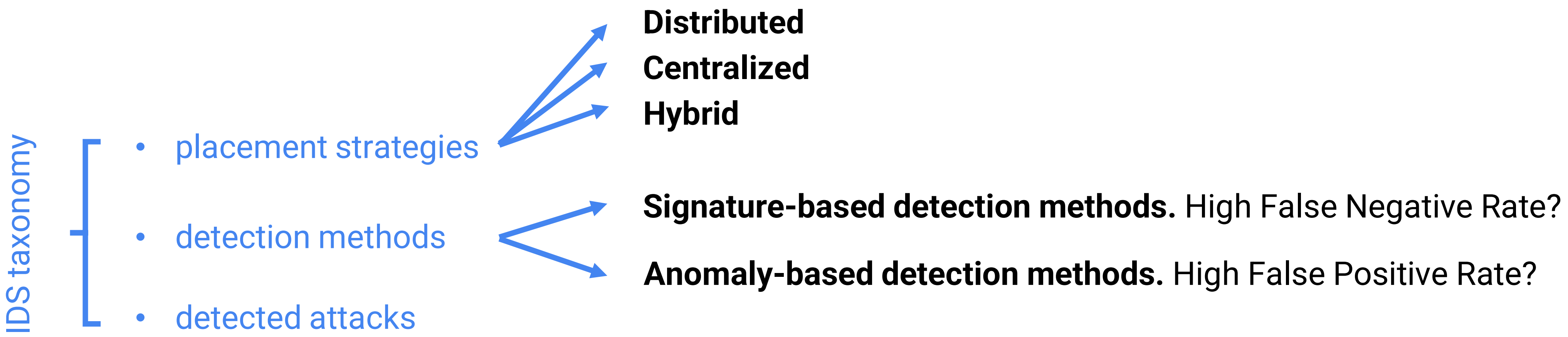
Logs Alarms

HIDS (Host IDS):

- host low resources and OS conformation,
- access to fine data and side channel data.

NIDS (Network IDS):

- effective or furtive network node, in a more powerful device,
- access to addresses, frames type, payload, etc… until cyphered.



IDS taxonomy

- placement strategies
- detection methods
- detected attacks

Distributed

Centralized

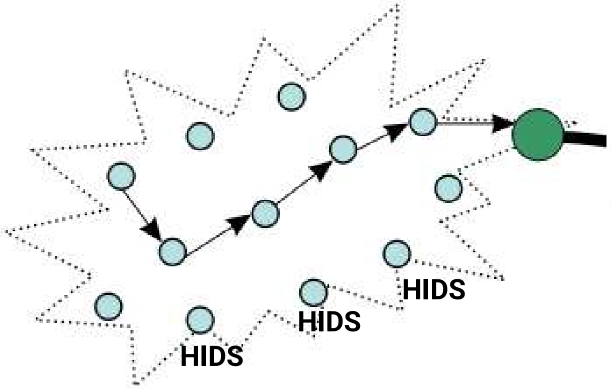
Hybrid

Signature-based detection methods. High False Negative Rate?

Anomaly-based detection methods. High False Positive Rate?

(Zarpelão et al., 2017)

2 - IDS in a nutshell > a few IDS examples

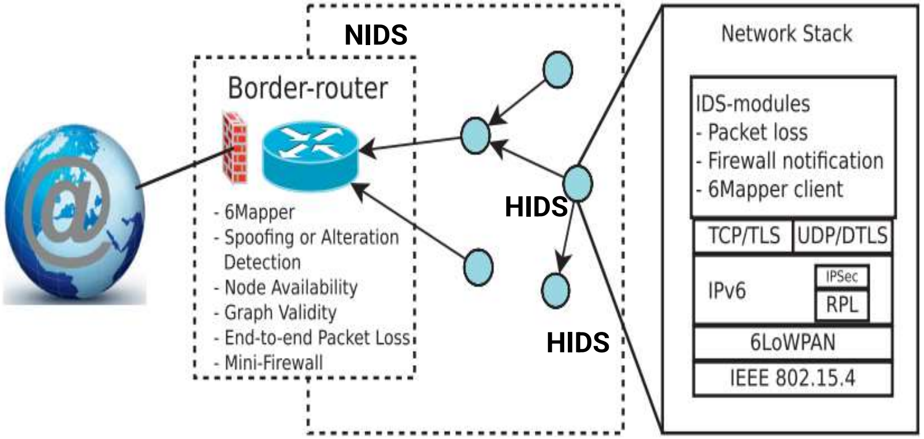


(Lee et al., 2013)

Distributed placement

Anomaly-based detection
Host actual electrical consumption is compared to a modelized consumption.

Detected attacks
DoS attacks in 6LoWPAN contexts.

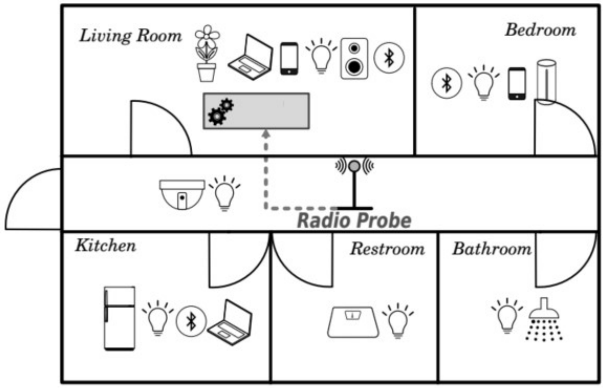


(Raza et al., 2013)

Hybrid placement
HIDSs cooperate with the NIDS to elaborate a network graph used in intrusion detection.

Hybrid detection (signature & anomaly)

Detected attacks
Routing attacks in 6LoWPAN contexts.



(Roux et al., 2018)

Centralized placement, furtive NIDS

Anomaly-based detection
RSSI* captured by radio probe feeds an autoencoder neural network previously trained with normal situations.

Detected attacks
Several, in several protocol stacks.

**Received Signal Strength Indication*

3 – Characteristics of a smart-home IDS

Many IDS papers do not address protocol stacks heterogeneity (neither cost nor user profile)

A few papers started addressing it: (Siby et al., 2017), (Roux et al., 2018), (Anantharaman et al., 2020), (Tournier et al., 2020)

Requirements of a smart-home protection solution:

- coverage of most popular technologies and new ones,
- adapted cost (<100 €),
- standalone in already deployed sites, simple for users.

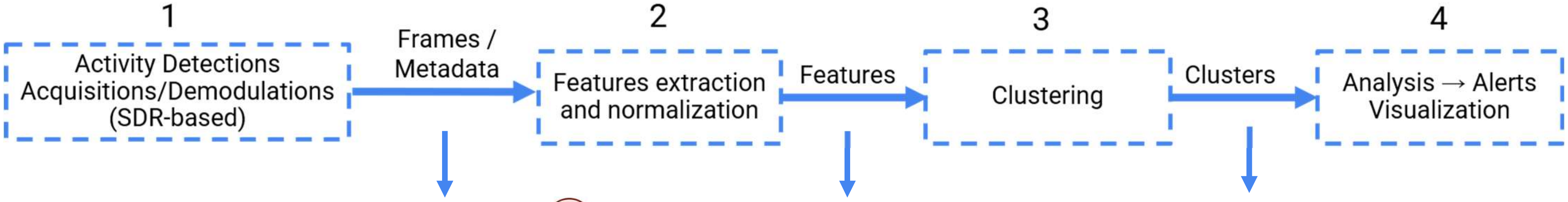
Requirements
x
IDS taxonomy

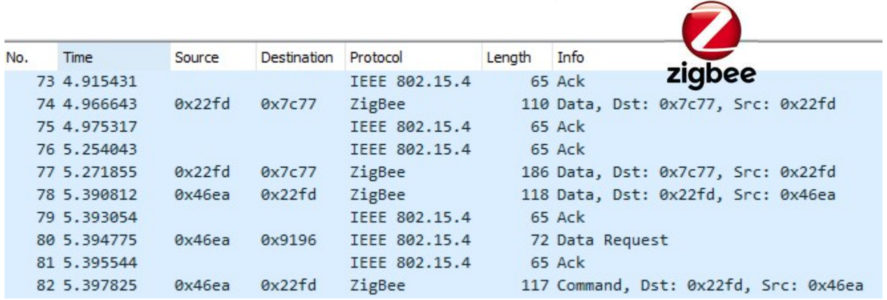
- centralized NIDS with medium resources, updatable,
- anomaly-based, cheap unsupervised ML algo,
- agnostic, passive, autonomous,
- polyvalent architecture thanks to agnostic SDR* probe(s),
- alerts performed by relevant smartphone notifications.

Software-Defined Radio

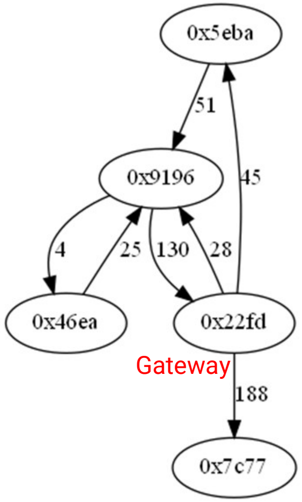
3 – Proposed architecture for a smart-home IDS

A « passive, low-cost and easy to use multi-stack centralized IDS »

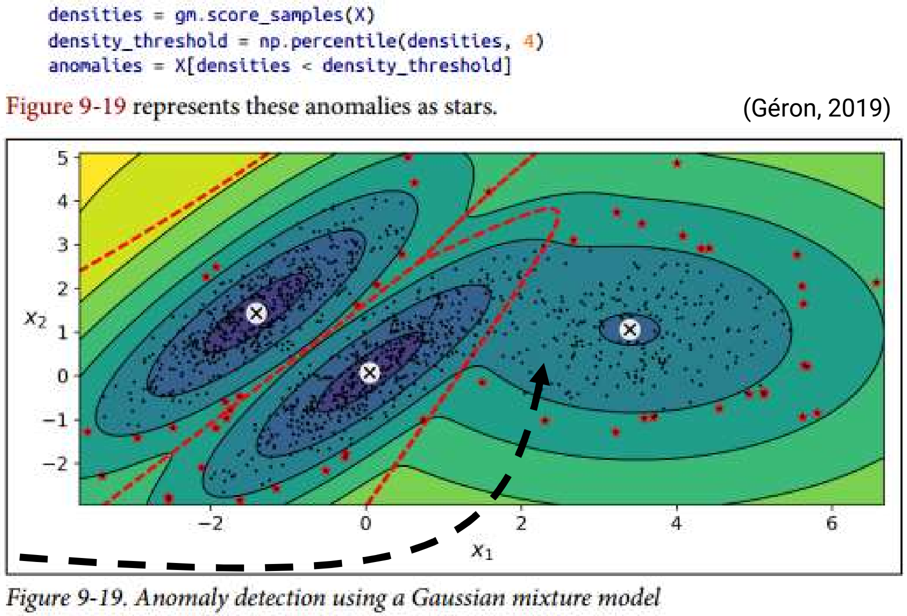




No.	Time	Source	Destination	Protocol	Length	Info
73	4.915431			IEEE 802.15.4	65	Ack
74	4.966643	0x22fd	0x7c77	ZigBee	110	Data, Dst: 0x7c77, Src: 0x22fd
75	4.975317			IEEE 802.15.4	65	Ack
76	5.254043			IEEE 802.15.4	65	Ack
77	5.271855	0x22fd	0x7c77	ZigBee	186	Data, Dst: 0x7c77, Src: 0x22fd
78	5.390812	0x46ea	0x22fd	ZigBee	118	Data, Dst: 0x22fd, Src: 0x46ea
79	5.393054			IEEE 802.15.4	65	Ack
80	5.394775	0x46ea	0x9196	IEEE 802.15.4	72	Data Request
81	5.395544			IEEE 802.15.4	65	Ack
82	5.397825	0x46ea	0x22fd	ZigBee	117	Command, Dst: 0x22fd, Src: 0x46ea



60-second graph w./ number of frames between nodes



```
densities = gm.score_samples(X)
density_threshold = np.percentile(densities, 4)
anomalies = X[densities < density_threshold]
```

Figure 9-19 represents these anomalies as stars.

Figure 9-19. Anomaly detection using a Gaussian mixture model

(Géron, 2019)

Conclusion

Contribution

- a smart-home IDS design based on smart-home ecosystem characteristics: tech., economical, human.

Open questions

- radio conditions: signal strength, coverage, etc. : number/localization of probes ?
- dimensionality of data/graphs.

Roadmap

- end up workflow for Zigbee (to date: steps 1 & 2 of architecture are completed),
- assess workflow relevance with malware datasets or real attacks,
- support another protocol stack → successful POC of an IDS to be adopted in smart home contexts.

Thank you for your attention.

`olivier.lourme@univ-lille.fr`

References

Alrawi, O., Lever, C., Antonakakis, M., Monrose, F., 2019. SoK: Security Evaluation of Home-Based IoT Deployments, in: 2019 IEEE Symposium on Security and Privacy (SP). Presented at the 2019 IEEE Symposium on Security and Privacy (SP), pp. 1362–1380. https://doi.org/10.1109/SP.2019.00013

Anantharaman, P., Song, L., Agadakos, I., Ciocarlie, G., Copos, B., Lindqvist, U., Locasto, M.E., 2020. IoTHound: environment-agnostic device identification and monitoring, in: Proceedings of the 10th International Conference on the Internet of Things, IoT ’20. Association for Computing Machinery, New York, NY, USA, pp. 1–9. https://doi.org/10.1145/3410992.3410993

Dhanjani, N., 2015. Abusing the Internet of Things [Book] [WWW Document]. URL https://www.oreilly.com/library/view/abusing-the-internet/9781491902899/ (accessed 6.30.20).

ENISA, 2017. Baseline Security Recommendations for IoT [WWW Document]. URL https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot (accessed 5.9.20).

Géron, A., 2019. Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow, 2nd Edition [Book]. O’REILLY.

Khandelwal, S., 2018. Z-Wave Downgrade Attack Left Over 100 Million IoT Devices Open to Hackers [WWW Document]. The Hacker News. URL https://thehackernews.com/2018/05/z-wave-wireless-hacking.html (accessed 7.11.20).

Kolias, C., Kambourakis, G., Stavrou, A., Voas, J., 2017. DDoS in the IoT: Mirai and Other Botnets. Computer 50, 80–84. https://doi.org/10.1109/MC.2017.201

Lee, T.-H., Wen, C.-H., Chang, L.-H., Chiang, H.-S., Hsieh, M.-C., 2014. A Lightweight Intrusion Detection Scheme Based on Energy Consumption Analysis in 6LowPAN, in: Huang, Y.-M., Chao, H.-C., Deng, D.-J., Park, J.J. (Jong H. (Eds.), Advanced Technologies, Embedded and Multimedia for Human-Centric Computing, Lecture Notes in Electrical Engineering. Springer Netherlands, Dordrecht, pp. 1205–1213. https://doi.org/10.1007/978-94-007-7262-5_137

Lueth, K.L., 2018. State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating. URL https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/ (accessed 11.17.20).

Raza, S., Wallgren, L., Voigt, T., 2013. SVELTE: Real-time intrusion detection in the Internet of Things. Ad Hoc Networks 11, 2661–2674. https://doi.org/10.1016/j.adhoc.2013.04.014

Roux, J., Alata, E., Auriol, G., Kaâniche, M., Nicomette, V., Cayre, R., 2018. RadIoT: Radio Communications Intrusion Detection for IoT - A Protocol Independent Approach, in: 2018 IEEE 17th International Symposium on Network Computing and Applications (NCA). Presented at the 2018 IEEE 17th International Symposium on Network Computing and Applications (NCA), pp. 1–8. https://doi.org/10.1109/NCA.2018.8548286

Siby, S., Maiti, R.R., Tippenhauer, N.O., 2017. IoTScanner: Detecting Privacy Threats in IoT Neighborhoods, in: Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security, IoTPTS ’17. Association for Computing Machinery, New York, NY, USA, pp. 23–30. https://doi.org/10.1145/3055245.3055253

Tournier, J., Lesueur, F., Mouël, F.L., Guyon, L., Ben-Hassine, H., 2020. IoTMap: A protocol-agnostic multi-layer system to detect application patterns in IoT networks 9.

Tschofenig, H., Baccelli, E., 2019. Cyberphysical Security for the Masses: A Survey of the Internet Protocol Suite for Internet of Things Security. IEEE Security Privacy 17, 47–57. https://doi.org/10.1109/MSEC.2019.2923973

Zarpelão, B.B., Miani, R.S., Kawakani, C.T., de Alvarenga, S.C., 2017. A survey of intrusion detection in Internet of Things. Journal of Network and Computer Applications 84, 25–37. https://doi.org/10.1016/j.jnca.2017.02.009

Zillner, T., 2016. ZigBee exploited - The good, the bad and the ugly. Magdeburger Journal zur Sicherheitsforschung 699–704.