The Ad hoc Semantic Internet Protocol (ASIP) for Constrained Devices

Kristina Sahlmann
HTW Berlin, University of Potsdam
Berlin, Germany
Email: sahlmann@htw-berlin.de

Thomas Schwotzer
HTW Berlin
Berlin, Germany
Email: thomas.schwotzer@htw-berlin.de

Bettina Schnor
University of Potsdam
Potsdam, Germany
Email: schnor@cs.uni-potsdam.de

***Abstract*—The relationship between Wireless Sensor Networks (WSN) and the Internet of Things (IoT) gets closer. The industry and masses are calling for simple solutions. We introduce the Ad hoc Semantic Internet Protocol (ASIP) to close this gap. It is an application layer protocol which allows direct communication between machines, peoples and both of them. It works ad hoc and has semantically annotated information. The ASIP protocol can be used not only for information exchange, but also for routing, network management and configuration, privacy and security, and even device maintenance.**

I. Introduction

The Internet of Things (IoT) consists of sensors and devices equipped with sensors which offer new features for the industry and mass deployment. Thus it is a kind of extended Wireless Sensor Network (WSN) with some special requirements. Much research work in WSN has been done, but new areas of research arise in context of IoT. Von Bodisco complains in his review about 20 years of sensor network research that complex and very specialized hardware and software was developed, and he calls for simple solutions in order to achieve cheap and flexible sensor networks for use in industry and private sector [1].

The requirements of IoT include the handling with constrained devices and constrained networks. The IETF has classified constrained devices in RFC 7228 [2]. Class 0 devices are very constrained devices like sensor-motes which are connected via gateway to the internet. Class 1 devices have less constrained capabilities in terms of power and processing units. Therefore they are able to run protocols like CoAP [3] and connect directly to the internet. Other constrained M2M protocols are e.g. 6LoWPAN [4] and MQTT [5].

Obviously there is a gap between traditional sensor networks and sensor-enabled constrained devices in IoT, as well as between the traditional web and sensor software development. Our proposal to close this gap is to add semantics to the traditional sensor network using the Ad-hoc Semantic Internet Protocol (ASIP). This protocol was developed in the recent project SharkNet[1] and the framework is open source[2]. Originally, it was designed for decentralized social networks. However, the ASIP protocol can also be applied for machines in the IoT, especially for the Semantic Web of Things (SWoT).

In this paper we introduce the basic message structure and functionality of ASIP. The exact description of the protocol is documented as Backus-Naur form[3].

II. ASIP Overview

ASIP is an application layer protocol. Thus it is independent of underlying protocols and physical layers and can also be applied to non-IP networks. The ASIP overlay network is built in a spontaneous way: ad-hoc and mobile, and each peer can connect to another peer in its neighborhood. In the following we use the terms peer, thing and device synonym. The protocol is asynchronous and stateless. The application logic defines when and how it responds on received data. Due to its routing capabilities via different criteria, the information in ASIP can be propagated to any peer.

Further, ASIP is a semantic protocol. The transferred information is semantically annotated. This makes the information self-explaining. The semantics can be used for filter and inference as well as for routing features. Furthermore, semantic annotations can be used for network building and configuration. ASIP is independent of the used vocabulary or ontology.

A. ASIP Data Structures

The ASIP data structures consist of interest and knowledge (see Figure 1). They can be used by any IoT devices (e.g. beacons, sensor-enabled devices, smartphones, etc.). An interest can have up to seven dimensions: topics, types, sender, approvers, receivers, times and locations. Additionally, an interest has a direction tag value. Direction describes whether a peer is willing to send (1), to receive (2) information or both (3).

A knowledge has the same dimensions as an interest. These dimensions describe the context of the information exchange. Additionally, information like text or values contains in the knowledge.

ASIP uses *Semantic Tags* for annotations. They could e.g. describe the temperature in degree Celsius. A semantic tag could have the name ”Temperature” and uses ”https://en.wikipedia.org/wiki/Celsius” as Subject Identifier (SI). SI was introduced by ISO 13250 Topic Maps. SI is a URI that refers

[1]http://sharedknowledge.github.io/
[2]https://github.com/SharedKnowledge/SharkFW
[3]https://github.com/SharedKnowledge/SharkFW/blob/master/asip.md

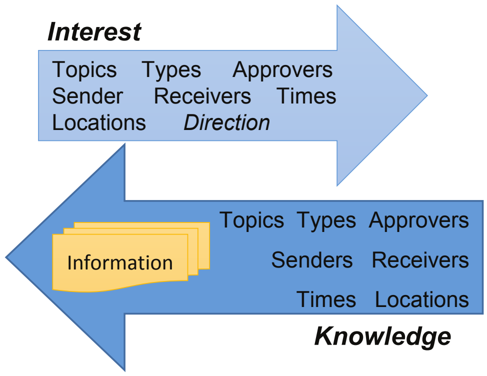


Fig. 1. ASIP data structures: interest and knowledge

a document on the web which explains tag's meaning. ASIP data structures use a subset of Topic Maps and RDF.

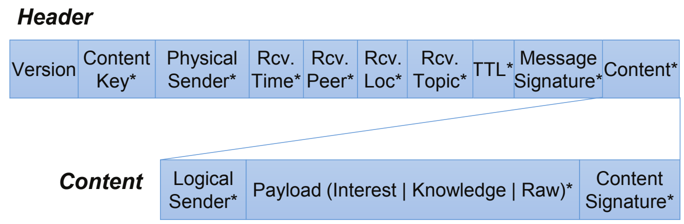
Besides simple Semantic Tags, there are three special Semantic Tags for peer, time and location. These tags have additional values besides name and SIs. The peer tag describes the resource, e.g. an IoT sensor-enabled device; the time tag captures a time frame or a moment, when the measurement took place; and the spatial tag describes the location, where the device is placed.

B. ASIP Message Structure and Routing Capabilities

Each ASIP message consists of a header and a content (see Figure 2). Summarizing, a header contains version, content key, physical sender; receiver time, peer, location, and topic; time to live (TTL), message signature. Except the version, all fields are optional. Technically, only a message containing the right version is a valid ASIP message.

Senders of a message are described by peer semantic tags. There are two sender fields: physical and logical. The physical sender is the actual device that sends this message, e.g. a Smartphone or a IoT device. The logical sender is described further below. Receivers can be described by four options and their combinations: time, peer, location, and topic. The optional receiving time describes time spans in which a message has to be arrived its receiver. The receiving peer can be described by a peer semantic tag and names the receiver of the content. Receiving location allows to describe a place on earth to which a message has to be sent. Finally, receiving topic allows to define a topic which can be used to describe the content or to set up things like subscription channels. A Time To Life (TTL) field is a positive integer number which should be decremented by every intermediate peer. A message should be discarded if TTL drops to zero. The whole message can be signed. It allows receivers to verify the sender's identity.

The content field consists of three optional parts: logical sender, payload and content signature. Logical sender is the originator of a payload. The ASIP payload can be an interest, knowledge or raw data. The payload can be signed and the signature will be sent with the message itself. Furthermore, the content can be encrypted by the Advanced Encryption Standard (AES). The AES content key is RSA encrypted with



* These fields are optional

Fig. 2. ASIP message structure.

recipient's public key and sent within the header. If TLS is supported by both peers, this is the preferred option for message encryption.

The receiver data in a header is used for routing features for scalability. ASIP has several routing possibilities: by peer (ASIP-PR), topic (ASIP-TR), location (ASIP-SR), gossip (ASIP-GR), and the combination of gossip and topic routing (ASIP-GTR). ASIP-PR routes the message to the addressed peer which is defined by semantic peer tag. ASIP-TR is based on the receiver's topic which describes peer's interests. Several peers can be interested in the same topics and therefore receive and use this message. ASIP-SR is based on receiver's location. Messages can be routed towards a receiver's place on earth, based on the Open Geospatial Consortium (OGC) simple feature model[4]. ASIP-GR is gossiping (compare to [7]) the message to everyone using TTL. The initial value of TTL can be specified by an application. The reasonable starting value for IoT applications is a topic of further research. Finally, ASIP-GTR combines routing by gossip and topic. Peers process messages which contain only interesting topics. Otherwise they will be passed to other peers in the gossiping way.

C. ASIP Functionality and Other Protocols

In this section we describe the basic functionality of ASIP and compare it with existing protocols.

The ASIP message exchange bases on only two structures: interest and knowledge. A simple example is shown in Figure 3. The communication between two things starts with sending an interest. Let's assume device C is interested in a peer which is collecting humidity values. Device C connects to device B, because it is in the neighborhood, and sends its interest to device B. B has a temperature sensor and does not have an interest in getting humidity values. Therefore, B returns its own interest to C. Later device A connects B and asks it for humidity and temperature. B answers with knowledge of the current temperature and of the peer C for humidity. Now A knows C through B and sends an interest for humidity directly to C. C responds with the current humidity value to device A. This scenario uses B as a *broker*.

Comparing with other protocols, ASIP is an application layer protocol and independent of the underlying layers (see Figure 4). It can adopt any transporting protocol in a modular

[4]http://www.opengeospatial.org/standards/sfa

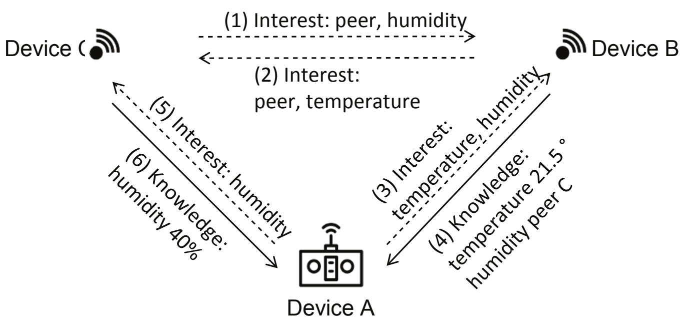


Fig. 3. ASIP scenario example

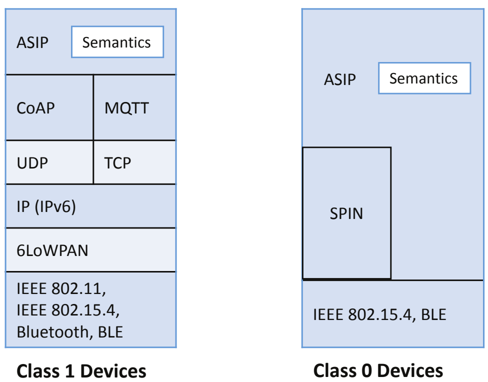


Fig. 4. ASIP in OSI Reference Model

way. Our current prototype uses TPC via Wi-Fi Direct and Bluetooth Low Energy.

Furthermore, semantics is already included as part of the protocol in contrast to other protocols. ASIP uses a subset of ISO 13250 Topics Maps and RDF, but it is independent of the used vocabulary. This has an advantage to evaluate data directly using known technologies.

The common architectures of the IoT solutions base e.g. on MQTT or CoAP protocol and connect to the cloud. We can use ASIP on top or even instead of these protocols for Class 1 devices. On the other side we can use ASIP as L3 protocol for Class 0 devices. The routing in Wireless Sensor Networks(WSN) was surveyed in [8]. The SPIN protocol [9] and ASIP are related in their routing functionality, but SPIN does not define a format for meta-data. A further topic for research is whether SPIN can be reused for routing or ASIP itself is the better solution in the IoT.

Mineraud requires in [10] an IoT platform which can access to a pool of standardized communication protocols and device manufacturer may select the appropriate protocols (e.g., CoAP for constrained devices). ASIP can fulfill it by deploying on devices and hiding the underlying protocols.

ASIP was designed with IoT in mind and thing-to-thing communication. Therefore it is a possible solution for an interoperable IoT.

III. Related Work

Petersen et al. emphasize in [11] that densely deployed IoT devices and local interaction between them will leverage not only traditional infrastructure-based network paradigms, but also spontaneous wireless network paradigms where devices may dynamically self-organize the relaying of data towards destinations without the help of infrastructure and pre-provisioned access points. Spontaneous wireless networks can be build on top of IEEE 802.11 ad hoc mode or IEEE 802.15.4, for example.

IETF established a research group ”Thing-to-Thing (t2trg)”[5] to investigate an Internet where low-resource nodes (e.g. constrained devices) can communicate with each other and with the Internet. We contribute with ASIP towards this research.

IV. Conclusion

This paper gives an overview of the main features of ASIP and shows similarities between the IoT and WSNs. The current implementation of ASIP is implemented using WLAN and Bluetooth for smartphones. Our next step, is a prototype implementation for constrained devices and networks. Further, we want to compare the ASIP approach with domain specific solutions like SensorML[6] and the Sensor Web Enablement Services[7]. The results will be included in the presentation.

Acknowledgment

This research is funded by the Federal Ministry of Education and Research under grant number Professors Program II. The responsibility for the content of this publication lies with the authors.

References

[1] A. von Bodisco, “20 Jahre Sensornetze-Praxisorientierte Forschung?” in *14. GI/ITG KuVS Fachgespräch Sensornetze*, D. Eckhoff, Ed., Erlangen, 2015, pp. 33–36.

[2] C. Bormann, M. Ersue, and A. Keranen, “RFC 7228 - Terminology for Constrained-Node Networks,” 2014.

[3] Z. Shelby, K. Hartke, and C. Bormann, “RFC 7252 - The Constrained Application Protocol (CoAP),” 2014. [Online]. Available: https://tools.ietf.org/html/rfc7252

[4] N. Kushalnagar, G. Montenegro, D. Culler, and Hui, W, Jonathan, “RFC 4944 - Transmission of IPv6 Packets over IEEE 802.15.4 Networks,” 2007. [Online]. Available: http://tools.ietf.org/html/rfc4944

[5] A. Banks and R. Gupta, “MQTT Version 3.1.1: Edited by Andrew Banks and Rahul Gupta. 29 October 2014. OASIS Standard. http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html. Latest version: http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/mqtt-v3.1.1.html.”

[6] T. Schwotzer, K. Sahlmann, and M. Schwarz, “Ad-hoc Semantic Internet Protocol (ASIP),” in *Submitted to: 8th EAI International Conference on Ad Hoc Networks*, Ottawa, Kanada, 2016.

[7] S. Jain, “Routing Techniques in Wireless Sensor Networks,” *International Journal of Computer Applications*, no. Volume 94 – No 6, May 2014, pp. 15–20, 2014.

[8] J. N. Al-Karaki and A. E. Kamal, “Routing techniques in wireless sensor networks: a survey,” *IEEE Wireless Communications*, vol. 11, no. 6, pp. 6–28, 2004.

[9] J. Kulik, W. Heinzelman, and H. Balakrishnan, “Negotiation-based protocols for disseminating information in wireless sensor networks,” *Wireless networks*, vol. 8, no. 2/3, pp. 169–185, 2002.

[10] J. Mineraud, O. Mazhelis, X. Su, and S. Tarkoma, “A gap analysis of Internet-of-Things platforms,” *Accepted for publication in: Computer Communications*, 2016.

[5] https://datatracker.ietf.org/group/t2trg/charter/
[6] http://www.opengeospatial.org/standards/sensorml
[7] http://www.opengeospatial.org/standards/swes

[11] H. Petersen, E. Baccelli, and M. Wählisch, "Interoperable Services on Constrained Devices in the Internet of Things," in *W3C Workshop on the Web of Things*, 2014. [Online]. Available: http://www.w3.org/2014/02/wot/papers/baccelli.pdf