Connecting Passive RFID Tags to the Internet of Things

Sandra Dominikus and Jörn-Marc Schmidt
IAIK, Graz University of Technology
Email: firstname.lastname@iaik.tugraz.at

1 Introduction

The Internet of Things (IoT) is an upcoming topic as things getting smarter and are able to connect themselves with each other. One important point towards interoperability is to enable things to talk the same "language" to be able to interact with each other. As the "language" of the Internet is the Internet Protocol (IP), we suppose that enabling things to talk and understand IPv6 is a major step towards the implementation of the IoT.

The communication using IPv6 is especially a challenge for passive RFID tags that are equipped with limited resources only. However, even the computational power of such passive RFID tags increases rapidly. Modern tags are able to store and compute data, or even hold sensors. In order to draw advantage from this increased functionality, the integration into the IoT is essential. Powerful application scenarios can be developed when two-way communication with tags can be established via the network.

Hand in hand with the increasing functionality and the integration of RFID tags into networks arises the need for proper protection of the communication. This is a major topic, since we understand a node itself as a client in the network that should be able to communicate with other clients in a secure way. RFID-readers should play a role similar to routers: they are essential parts of the connection, but the clients do not need to trust them.

With this concept paper we want to show a method how to enable a two-way end-to-end communication with passive RFID tags via the Internet. Our method does not require much computational power on the tag side as the tag itself does not have to talk IPv6. We use the RFID readers as "translators".

2 Motivation and Concept

We want to establish a two-way communication between an RFID tag an a *Corresponding Node* in a network. Two-way communication means, that the tag can contact a *Corresponding Node* in the network at any time it is connected to the Internet and vice versa. We think of application scenarios where a *Corresponding Node* wants to change the tag status (e.g. revocation, call-back), write data on the tag (e.g. guarantee, maintenance), or poll the recent tag status (e.g. sensor data).

Our system consists of four communicating parties: the tag manager, the RFID readers, the tagged items, and so-called *Corresponding Nodes.* The tag manager issues the tags, i.e. personalization information is assigned to the tag, stores and manages information about the tags in a database. The intention of the *Corresponding Node* is to communicate with the tags to get information from it or to change information stored on the tag. In Figure 1 the communication processes between the parties are shown.

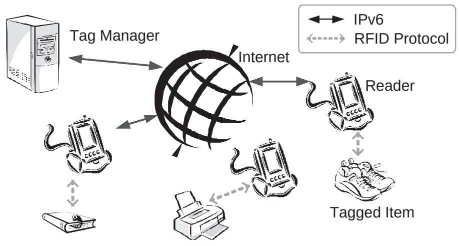

Figure 1: Communication Scenario

Tag Manager, RFID readers and *Corresponding Nodes* are connected to the Internet. The tagged items are mobile and are expected to move through different reader fields and "connect" to the readers via their standard RFID communication protocol.

The basic principle of this method is: The *Corresponding Node* sends a message with the IP address of the tag. The routing of this message is described in the next section. The message is delivered to the reader, where the tag is currently present. The RFID reader identifies the tag with the corresponding destination IP address and translates the message into RFID commands, which are sent to the tag. The answers of the tag are re-translated into IPv6 messages which are sent back to the corresponding node.

Mobile IPv6 (MIPv6) provides the routing and communication mechanisms for mobile nodes in the Internet and we want to use this concept for our so-called MIPv6-enabled tags. As shown in the figure, the passive tags are not able to do IPv6 on their own, but the readers do the work for them. In the next section we will describe this concept in detail.

3 Integration in the IoT

In our concept, the RFID tags do not implement the MIPv6 protocol by themselves but use the readers as a "translator" to the IPv6 network. Each tag holds a unique IP address and belongs to a tag manager. According to the MIPv6 terminology, we call this tag manager *Home Agent*.

When a tag is issued or newly assigned, the *Home Agent* creates a new item in a database, where all assigned tags are registered with their unique IDs (UIDs) and their *Home Addresses*. The *Home Address* is the tag's IP address and consists of the subnet prefix of the *Home Agent* and the tag identifier, which uniquely identifies the tag at the *Home Agent* site. If a tag enters a reader field, a *Care-Of Address* is created, which is the IP address where the tag can currently be reached. It consists of the subnet prefix of the reader, where the tag is currently located, and the tag identifier. This *Care-Of Address* is stored in the *Home Agent's* database to relay the communication to the current tag location.

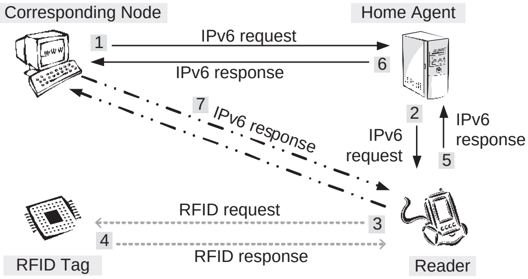

Figure 2: Communication Principle

Figure 2 shows the routing of a message from the *Corresponding Node* to the tag. The *Corresponding Node* sends a packet to the *Home Address* of the tag (1), i.e. it starts with the subnet prefix of the *Home Agent*. Therefore, the packet is sent to the *Home Agent* first. In its database, the *Home Agent* can derive the UID and the *Care-Of Address* of the tag. The IPv6 packet is forwarded to the *Care-Of Address* (2). The *Care-Of Address* refers to the subnet of the RFID reader, where the tag is currently present. The reader receives the IPv6 packet and sends the payload of the packet via an RFID request to the tag (3). The RFID response of the tag is translated into an IPv6 packet and sent back to the *Home Agent*(4)(5), which relays the packet to the *Corresponding Node* (6). Alternatively, the package is sent directly to the *Corresponding Node* with the *Care-Of address* as source address (7).

The reader acts as a router for the tags in its field. MIPv6-enabled tags indicate this feature with a flag in the inventory response. The reader obtains the *Home Address* from the tag and creates a new *Care-Of Address*: The subnet prefix of the *Home Address* is replaced by the subnet prefix of the reader. The reader derives the IP address of the *Home Agent* from the *Home Address* and sends the new *Care-Of Address* to the *Home Agent*.

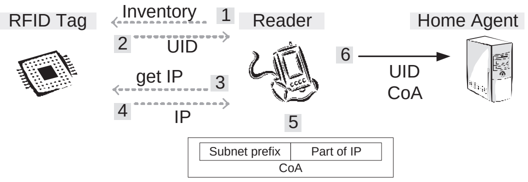

Figure 3: Address updating

Figure 3 shows the address-updating process. The reader performs a standard inventory command (1)(2). The tag indicates that it is MIPv6-enabled. The reader sends a *getIP* command (3) and receives the *Home Address* of the tag (4). The reader creates the new *Care-Of Address* for the tag (5) and sends it to the *Home Agent* (6). The *Home*

Agent updates its database with the new *Care-Of Address*. The reader adds the tag's *Care-Of Address* to a routing table. In [1], the concept is described in more detail.

The complexity of this system is shifted to the reader. The reader has to provide IPv6 router functionality and translation of the commands. It also controls the communication flow between the *Corresponding Node* and the tag. We assume that a reader has enough hardware resources available to handle these new requirements. RFID tags only need extra memory to store the IP address (128 bits) and two additional custom commands (e.g. *getIP* and *changeIP*).

4 Security Considerations

As we could observe in the "traditional" Internet, security was one of the major enabling techniques for many applications. Only by securing communications, Internet has become a trusted media. We believe the same will hold true for the Internet of Things. In the IoT, security will be even more important as things often act without the knowledge of the user. Securing IPv6 communications will work in the well known way by using IPSec, which is a protocol that provides authentication and confidentiality for an IP communication. Therefore, for the connection between IPv6 nodes (*Home Agent*, *Corresponding Node*, reader) security services are available.

The communication line between reader and MIPv6-enabled tag is not secured in a standard way. Passive RFID tags can already be cryptographically enhanced, they can already perform symmetric and asymmetric encryption algorithms (e.g. [2], [3], [4]). We propose to define a new security layer for the RFID communication between tag an reader in MIPv6 applications. For this purpose, security suites for tags shall be defined in order to provide different security mechanism, e.g. authentication or encryption. Each suite should define particular requirements for the tag (e.g. AES, SHA-1 and ECDSA) to fulfill the prerequisites for a standard security layer. The tag and the *Corresponding Node* have to agree on a suite to build up a secure connection. The reader only passes the content of the messages and can therefore disturb but not compromise the security of the end-to-end connection. The definition of these suites is out of scope of this concept, but is content of on-going research.

5 Conclusion

In this concept paper we describe a method to integrate passive RFID technology into the Internet of Things. We expect that this approach can be an enabling technology for many new applications with RFID tags. For our approach we apply concepts from MIPv6. The tags do not require IPv6 functionality themselves, but communicate with readers using their standard RFID communication protocol. The readers provide MIPv6 functionality and act as gateway between the Internet and the tags.

Most additional overhead for the required operations accumulates on the reader side, as typical RFID readers provide enough computational power to implement such additional functionality. We shortly discuss the concept of security suites for the remote RFID communication to set up a secure communication. We can conclude that MIPv6 allows to fully integrate passive RFID tags into the IoT in a transparent and compatible way, while the question of a secure connection is still under research.

References

[1] S. Dominikus, M. J. Aigner, and S. Kraxberger. Passive RFID Technology for the Internet of Things. In *Workshop on RFID / USN Security and Cryptography*, 2010.

[2] M. Feldhofer, J. Wolkerstorfer, and V. Rijmen. AES Implementation on a Grain of Sand. *IEE Proceedings on Information Security*, 2005.

[3] D. Hein, J. Wolkerstorfer, , and N. Felber. ECC is Ready for RFID - A Proof in Silicon. In *Workshop on RFID Security 2008 (RFIDsec08)*, July 2008.

[4] M. Hutter, M. Feldhofer, and T. Plos. An ECDSA Processor for RFID Authentication. In *Workshop on RFID Security (RFIDsec 2010)*, June 2010.