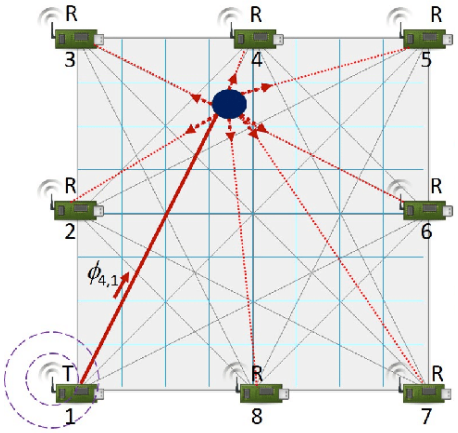
TechInf
Institut für Technische Informatik

RI CODE Research Institute Cyber Defence
Universität der Bundeswehr München

Indoor Localization without GPS under RIOT OS (BA/MA)

Over several years a big IoT network called SecureWSN was established and continuously expended towards a trustworthy environmental monitoring framework for constrained networks. The network itself consists of 3 parts: (1) Data collection via constrained devices, (2) gateway component handling incoming data and managing the network called CoMaDa, and (3) a framework realizing backend and front-end for the end-user called WebMaDa. Several theses are available in those parts of SecureWSN.

In the current application scenario Smart Home it is assumed that the network owner knows where he/she placed the nodes during the deployment phase. But in reality we become forgetful, disguise things or hide them unintentionally. This causes a problem as soon as we need to get in physical contact to the device or need to verify its correct work. The obvious solution here would be localization by GPS, but this is very difficult indoors for well-known reasons, and in our case it is not possible because the nodes do not have GPS modules.



Therefore, the scope of this thesis is to design and develop a location approach without the classic approach using triangulation over GPS-coordinates. Further it is assumed to reuse existing features and structures of SecureWSN (e.g., data format of TinyIPFIX and eavesdropped information). In order to face the location problem the following steps are required:

- Checkout possibilities to locate devices (what are general strategies),
- Decide what strategy is the best for the assumed scenario and reuse existing protocols or functions,
- Specify the workflow and the communication concept,
- Implement the location procedure, and
- Include it in the existing framework
    - Giving the network owner an option to receive the information of the location (e.g., GUI or messaging),
    - Modify the existing database with required tables and procedures,
    - Ensure respecting the privilege strategy (meaning this feature is only available for network owner), and
    - Ensure that all existing features still functioning.

Finally, the complete solution needs to be evaluated in a proof-of-operation manner and the report needs to be written. Further, a detailed documentation on how to install the solution in the existing infrastructure is required. Depending on the chosen thesis type the content will be adapted in its complexity. Depending on the results we will try to publish it on high ranked conferences and workshops.

As this work is based on different works and research results, a willingness to familiarize oneself with the existing system is expected. Knowledge of database structures (especially MySQL) and front/backend programming (i.e. Java, C, PHP, Docker) as well as node programming under RIOT OS would be an advantage.

We will offer you access to existing installations of SecureWSN's components and written theses of SecureWSN as well as a smart working environment and deep contact to supervisors and a lot of discussions and knowledge exchange within out IoT-Roundtable.

If you are interested in this thesis, contact us and let's discuss:

- PD Dr. Corinna Schmitt (UniBW, Examiner at the LMU), Email: corinna.schmitt@unibw.de