Secure Data Transmission in Constrained Networks (several BAs/MAs are possible)

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.

As any data collected includes sensitive information (e.g., IP address, GPS information, ID) data transfer in a networks needs to be secured. Therefore, manifold approaches exist, which are in general challenging for resource-constrained devices. This means, special solutions must be designed and implemented fitting the requirements (e.g., limited power, limited computation capacity, and memory), but still running the essential application.
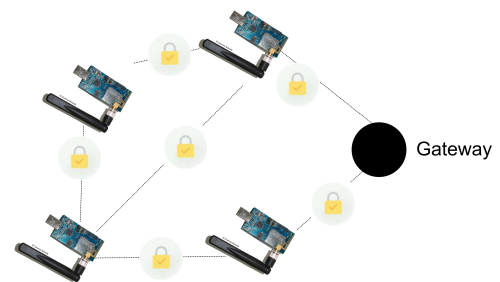
Thus, this thesis looks for a resource-efficient implementation of a protocol in the collection network securing the communication towards the gateway. Currently the most powerful platform in place is OpenMote B running RIOT OS. Therefore, we are looking for:
- Pre-shared key approaches and
- Advanced approaches

Keep in mind, the opportunities are manifold and YOU can decide which one you like to investigate!

The following things are requested to be designed, implemented, and evaluated (most likely via proof-of-concept) in this thesis:
- Security algorithm itself
- Integration and support into SecureWSN
    - Configuration and deployment
    - Decoding and encryption on necessary places (e.g., gateway or aggregator) and forwarding payload into the backend

Finally, the report needs to be written, as well as a detailed documentation and handing over a running VM with the complete project with all sources. Depending on the chosen thesis type the content will be adapted in its complexity. Depending of the results we will try to publish it on high ranked conferences and workshops.

Knowledge in C/C++ programming and little bit SQL, PHP, JavaScript would be an advantage.

We will offer you:
- Access to existing source code in different operating systems (TinyOS, Contiki, RIOT OS)
- Access to written theses in the project SecureWSN
- Virtual machine running Ubuntu and CoMaDa including a link to WebMaDa and the backend
- Initial literature
- Smart working environment
- Deep contact to supervisors and a lot of discussions and knowledge exchange

As this work is based on different works and research results, a willingness to familiarize oneself with the existing system is expected. Based on the results of the work, further work will be put out to tender, so that detailed documentation is required at all levels, as well as close cooperation with the supervisors.

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

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