Privacy and security in Body Area Networks

Directeur de thèse : Maria Potop-Butucaru (LIP6, **maria.potop-butucaru@lip6.fr**)

Encadrant : Claude Chaudet (claude.chaudet@enst.fr)

Domaine: Sciences et technologies de l'information et de la communication

Projet

The rapid advances in sensors and ultra-low power wireless communication has enabled a new generation of Wireless Sensor Networks (WSN). Wireless Body Area Networks (WBAN) open an interdisciplinary area within WSN research, in which sensors are used to monitor, collect and transmit medical signs and other measurements of body parameters. The intelligent sensors can be integrated into clothes (wearable WBANs), or placed directly on or inside a body. If typical applications target personalized, predictive, preventive and participatory healthcare, WBANs also have interesting applications in military, security, sports and gaming fields. Care workers, for instance, are really in demand of systems that permit a continuous monitoring of elderly people or patients to support them in their daily life. WBANs history is just at its beginning, and many news and improvements are expected in the next future. Body Area Networks differ from typical large-scale wireless sensor networks in many aspects. The characteristics of the wireless channel are different. Links have, in general, a limited range, a low quality and vary over time due to posture mobility. Besides, the effect of body absorption, reflections and interference cannot be neglected. For these reasons a direct link (one-hop) between the data collection point and the other nodes is very difficult to maintain while keeping a low transmission power.

Security and privacy are important challenges, even more than in classical sensor networks considering the sensitivity of the collected data. The environment is even more constrained: the devices cannot embed an AA battery and computation and commutation need to be even further limited. This poses serious challenges for security and privacy, as most of the state of the art techniques rely on cryptographic algorithms, most of which are computationally intensive. BAN have other specificities, such as a very limited transmission range or a constrained mobility that has some pseudo-periodic components. These specificities can either be considered as limitations, or be utilized. The transmission range, for instance, can be limited to restrict access to data to close nodes (i.e. within visibility range) to compensate weaknesses of low-complexity cryptography. Mobility can also be utilized to pair nodes and detect unauthorized nodes.

Enjeux

Security and privacy in this area are an important challenge. That is, when low power nodes exchange data some of the cryptographic schemes and security tools cannot be used as they are. Also nodes are more vulnerable to internal and external attacks.
We propose to investigate the best effort algorithmic and protocolar solutions for ensuring the security and the privacy of the medical data while guaranteeing low energy consumption, such that the network lifetime is long (month, years) even though on-body sensors are equipped only with a little battery.