Security and Reliability in Wireless Body Area Networks for Healthcare

Mots clés :
- Directeur de thèse : ahmed MEHAOUA
- Co-encadrant(s) :
- Unité de recherche : Laboratoire d'Informatique PARis DEscartes
- École doctorale : École Doctorale Informatique, Télécommunications, Électronique de Paris
- Domaine scientifique principal: Divers

Résumé du projet de recherche (Langue 1)

Today, healthcare professionals and caregivers are very interested in remote monitoring of elderly people and patient vital signs, as well as their surrounding environment. These requirements have sparked enormous interest in the utilization of Wireless Sensor Networks (WSNs). Scientists and researchers have developed networks of wireless sensors, known as Wireless Body Area Networks (WBANs), which are composed of a set of small miniaturized sensors with wireless transmission capabilities, and may be externally attached or implanted. These devices are used to continuously gather physiological signals from patients or elderly people at home or in hospitals, and transmit collected data to a Local Processing Unit (LPU) such as a smartphone or tablet. There exist many medical WBAN systems which are publicly available for purchase including MICAz, MICA2, Tmote Sky, TelosB, IRIS, Imote2, and Shimmer. These types of WBANs are used to monitor and collect various physiological parameters of individuals such as Heart Rate (HR), pulse, oxygen saturation (SpO2), Respiration Rate (RR), Body Temperature (BT), ElectroCardioGram (ECG), ElectroMyoGram (EMG), Blood Pressure (BP), Blood Glucose Levels (BGL), Galvanic Skin Response (GSR), etc. The use of WBANs has been extended to monitor patients diagnosed with chronic illnesses and cognitive disorders such as Parkinson's, Diabetes, Alzheimer's, Asthma, and Epilepsy. WBANs have proven to be great assets to both patients and healthcare providers. While WBANs have numerous advantages, their disadvantages range from poor reliability to the high susceptibility of security attacks after deployment. WBAN sensor nodes are prone to both hardware and software issues such as impaired components, sensor calibration, battery exhaustion or dislocation. The sensor readings are themselves both unreliable and inaccurate [1-8]. Individual sensor data gathering and transmission is also prone to several types of irregularities such as interference, noise, sensor misplacement, sweating patients, exhausted energy resources and external hacks and malevolent attacks such as data injection, modification or replay attacks that indirectly affect the LPU. This may lead to unexpected results, faulty alarms and inaccurate diagnosis results, and consequently reduction in public trust of these systems.

Résumé du projet de recherche (Langue 2)

Informations complémentaires (Langue 1)
This research activity will be in collaboration with three research groups from USA (Florida Atlantic University) and China (Beijing Univ. of Post and Telecommunications. Some visits will be planned during the PhD thesis period.

Informations complémentaires (Langue 2)
Required Skills: - Sensor networks hardware and software architectures (TinyOS,NesC, etc.) - Anomaly Detection - Security - ZigBee/Bluetooth/802.15.4 - Machine Learning and Data Mining - Decision Theory - Statistical data analysis. Programming skills in C/C++, MatLab, TinyOS/NestC. Writing in english, autonomy and initiative.