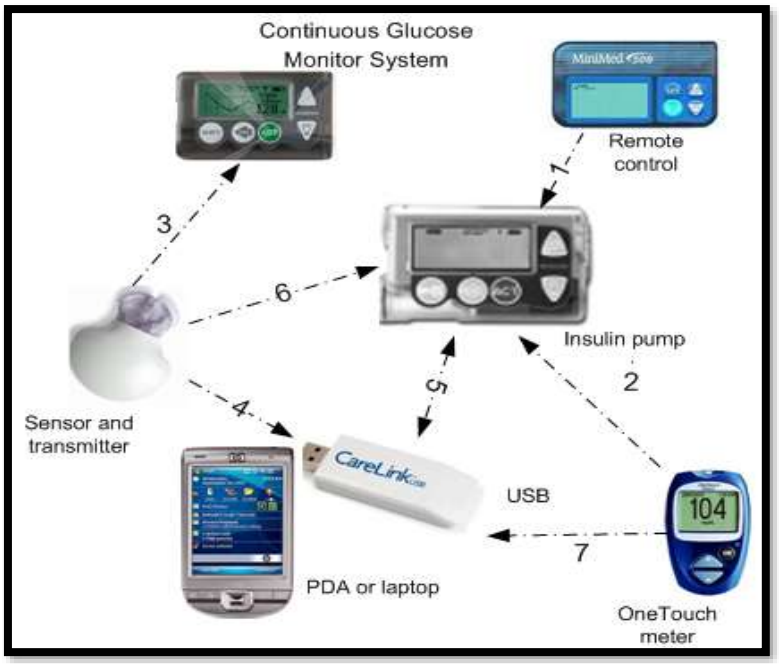
Reference source not found.. Many medical devices have much less resources than wireless sensor nodes. Hence, security schemes designed for sensors are not suitable for most of these medical devices.

Second, existing pre-shared-key-based security schemes do not work well for medical devices. A pre-shared-key-based security scheme let two devices pre-share a secret key, thus the communication between the two devices can be secured. This kind of security schemes have been widely used for security in wireless sensor networks as well as other wireless networks. However, this approach does not work well for implantable medical devices, even though some may have the resource to run crypto algorithms. For a medical device, if it has a pre-shared key with a reader/controller, the key may be used to run security operations. However, a pre-shared key will bond a medical device to a particular reader. This means that if the patient is out of town and goes to see a different doctor who does not have the key, there is no way to authenticate and communicate. Storing the key in an online server will have some problems: (1) a reader may not have Internet access at all times, and (2) it is expensive to run and keep up a global online server. Hence, this approach does not work well for tiny medical devices.

Third, security schemes for medical devices should be able to handle patients' emergency situations. During an emergency (a coma for instance), a patient may be unconscious and cannot provide the required credentials (such as a security key or a token) to the medical personnel, nor can the patient tell the doctor about his/her medical condition. In addition, neither device-based schemes nor family-based schemes can be used if the patient has an emergency outside his home city/country. In this case, the patient's safety outweighs the security concerns of medical devices. A good security scheme should satisfy security, privacy and safety requirements.



To mitigate some of the above challenges, we got an NPRP project to study this situation and come up with potential solutions. After which we embarked on developing (1) a general data analytic approaches and models of medical data as well as proof-of-concept security schemes for medical devices. We collaborated with medical hospitals that provided us with real medical device data. Using this data allowed us to develop proof-of-concept security schemes for these devices; (2) we designed effective security schemes for patients in emergency situations. For the above two cases, we used the system shown in the Figure referring to an Insulin Pump System. Finally and in order to generalize our findings, we developed effective security schemes for the general purpose wireless medical devices.

This project was a great success in terms of publications and the developed prototypes. A total of 11 journal publications and 13 conference papers were accomplished. Members of the team from our department are: Prof. Amr Mohamed, Dr. Abdulla Al-Ali and Prof. Mohsen Guizani. The outside collaborator was at Temple University in the USA represented by Prof. James Du as the PI. For more information on the research details and the achievements of this project, readers are referred to the publications available online.