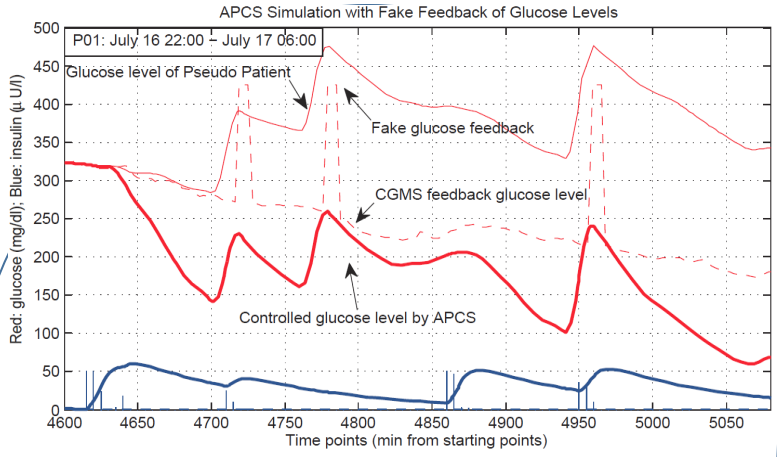
Cyber-Physical System Security in Implantable Insulin Injection Systems

Challenge:

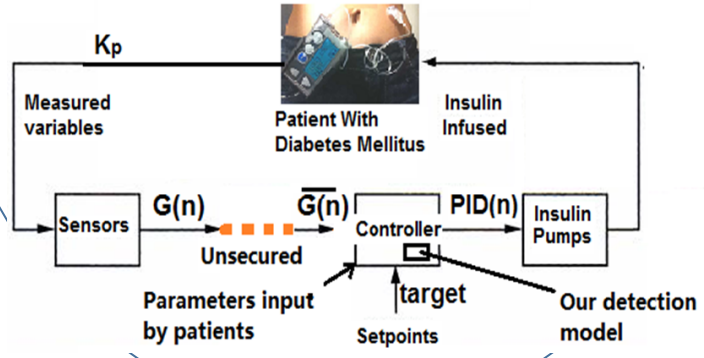
- Glucose level of a patient is personalized, time-sensitive, high related to patient's food flavor and life style.
- How to detect and defend against glucose level attack?



(b) Glucose level attack 1

Solution:

- Abnormal glucose level attack detection: A mathematical model to calculate the expected glucose level based on patient physiological parameters
- Out of band secure channels
- Investigate several new types CPS attacks



Glucose level attacks Detection model

Scientific Impact:

- Expand the research frontier in analogy security by exploring side-hiding technology in wireless artificial pancreas.
- Addresses the design questions of how to detect and defend against the jamming attacks and fake glucose sensor readings.
- Expose more vulnerabilities in wireless insulin injection system.

Broader Impact:

- Multiple efforts will facilitate the large-scale deployment of our results including potential collaboration with manufacturers of wireless medical devices.
- Millions diabetes using pumps will care about the research results.
- Support 1-2 minority undergraduates and a security workshop for male minority middle school students
- Collaborations with Upenn, UA, UD, and other universities around.

CNS-1566166 (PI: Xiali (Sharon) Hei, Delaware State university, xhei@desu.edu, 3028577446)