Securing Sensor Networks

Students: Saharnaz ZareAfifi and Romil Verma
Adviser: Brian King (ECE)
Purdue School of Engineering & Technology
Indiana University – Purdue University Indianapolis

Abstract

Sensors can have significant impact on one's life. They can measure temperature, level of humidity, speed, motion, distance, light or the presence/absence of an object and many other phenomena and then these measurements can be processed together to provide the information that we use to make informative decisions. Today with the use of smart devices, such as iPhone, android phones, etc, we can interface with these sensors and use them in our daily lives. In the future, we will encounter even more intelligent and precise sensors, some that can significantly change our society. For example, consider sensors which can track eye movements and then process these movements to move the cursor within a windows session on a computer [1], envision how this could impact a paraplegic or even be applied within a computer aided surgical unit. Consider future sensors that can analyze the protein contents of a single cell and how they can be used in applications for medical diagnosis [2] or sensors that allow you to track and modify your energy usage [3]. Again, a potential conduit to these sensors may be our smart devices. In general, these sensors will provide us data, for which we can make decisions that improve our lives. In the future these sensors will be interconnected, data will be collected, and processed and automated decisions will be made and implemented by our smart devices. If humans collect the data to make information, i.e. make decisions, then the human can intercede when they view the data is inaccurate, but if devices make automated decisions then such information/decisions will be limited by the accuracy of the sensor data. We cannot rely on faulty information generated by inaccurate data. Faulty data can be generated by sensors that are acting improperly, perhaps because of a consumed power source (i.e. battery) or by entities, i.e. malicious parties, who infuse false data into the sensor network. The potential of a malicious party within the sensor network exists, and in order for us to rely on the sensor data we must be able to detect faulty data as well as malicious behavior (possibly by the sensor device). In this research project we will explore several potential attacks to the sensor network. In this work, we will briefly discuss two security problems. First, if a sensor is sending faulty data then the information generated can be faulty. This information is usually characterized as data aggregation (the data from multiple sensors is aggregated into information) and such an attack is characterized as the Data Aggregation attack. In this project, we will explore methods to detect the Data Aggregation attack and develop countermeasures to protect against the attack. Secondly, because malicious parties (or sensors) may exist, there is a potential in an automated system, of one device accusing another device of inappropriate behavior. For example, a malicious device may accuse other devices to avoid detection. This type of attack is characterized as the Reputation attack. In this work we will discuss the Reputation and Data Aggregation attacks, and develop power friendly countermeasures (fewer complexes with small amount of calculation) to these attacks.

References

[1] "THE CITY OF THE FUTURE; AN INTERFACE REVOLUTION", http://www.laserfocusworld.com/news/2012/03/19/the-city-of-the-future-nl-an-interface-revolution.html, March 19,2012

[2]"Identity check" selectively screens single molecules passing through nanopores: IResearchers demonstrate versatility of solid-state protein sensor", http://insciences.org/article.php?article_id=10707

[3] Farhangi, H, "The path of the smart grid", IEEE Power and Energy Magazine, Vol 8 (1), pp. 18 - 28, Feb 2010