Probably wireless

September 3 2008

Wireless Sensor Networks (WSNs) used to detect and report events including hurricanes, earthquakes, and forest fires and for military surveillance and antiterrorist activities are prone to subterfuge. In the *International Journal of Security and Networks*, computer scientists at Florida Atlantic University describe a new antihacking system to protect WSNs.

Feng Li, Avinash Srinivasan, and Jie Wu explain that there are two types of cyber-sabotage that might occur on a WSN. The first is the fabricated report with false votes attack in which phony data is sent to the base station with forged validation. This presents the authorities monitoring a WSN for impending disaster with a quandary: if the data arriving from the network is validated but false, how can they know for sure?

The second kind of attack adds false validation votes to genuine incoming data. The problem facing those monitoring the WSN now is if genuine data is being labeled as false, how to trust any data arriving from the WSN.

Li and colleagues point out that most existing WSN systems have built-in software on the network that can ward off the first kind of attack so that false data usually cannot be given valid credentials and those monitoring the system will be able to spot subterfuge easily. However, WSNs are not usually protected against the second kind of attack, so that a genuine impending disaster cannot be verified remotely, which defeats the purpose of a WSN.

The team has now devised a Probabilistic Voting-based Filtering Scheme (PVFS) to deal with both of these attacks simultaneously. They used a general en-route filtering scheme that can achieve strong protection against hackers while maintaining normal filtering to make the WSN viable.

The scheme breaks WSNs into clusters, and locks each cluster to a particular data encryption key. As data reaches headquarters from the WSN clusters, the main cluster-heads along the path checks the report together with the votes, acting as the verification nodes in PVFS. The verification node is set up so that it will not drop a report immediately it finds a false vote, instead it will simply record the result. Only when the number of verified false votes reaches a designed threshold will a report be dropped.

This way, should a saboteur compromise one or more sensors on any given WSN to launch an attack, the PVFS will apply probability rules to determine the likelihood that this has happened. It will do so based on data arriving from other sensors in different clusters before reporting incoming data as false.

Detecting compromised sensors in a WSN in this way is of vital important to homeland security as well as successfully tracking natural events with the potential to devastate cities. By countering sabotage, false alarms that waste response efforts could be minimized in times of impending crisis.

Source: Inderscience Publishers