Title: An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks

Authors: Sencun Zhu, Sanjeev Setia, George mason University, Fairfax, VA
Sushil Jajodia, George mason University, Fairfax, VA; The MITRE Corporation, McLean, VA
Peng Ning, North Carolina State University, Raleigh

This paper talks about preventing data-injection compromises in a sensor network. Basically, the idea in this paper is to use a hop-by-hop authentication scheme, so that as long as a certain number of nodes aren't compromised, the base station will still know to reject/accept packets correctly. This is in contrast to many existing schemes where, when one node is compromised, the attacker can often carry out the intended attacks by injecting false data. Specifically, this is especially useful for non-numeric data where statistical aggregation isn't an option. Additionally, the systems strives to meet certain performance requirements, giving a "tradeoff between security and performance."

In general, the paper presents a very convincing case that the system accomplishes a few things. First, it prevents data injection attacks where fewer than a set number of nodes are compromised. Second, it has properties and protocols that allow it to fix or route around damaged or compromised nodes. Third, it can sit on top of sensor statistical data aggregation schemes, like those presented in other papers. It also gives the user some ability to choose the tradeoff between security and performance/power savings by letting the user implement a physical location check in the reporting via some locational system like GPS, at a performance and power cost.

However, there were some problems with the paper, largely in the assumptions and motivation. One of the bigger issues is the assumption that the sensors deployed will be deployed in such a way that more (hopefully, many more) than t nodes will all fall in a range small enough they they can communicate with each other. These nodes have to all be able to detect the same event, and must be able to communicate with the cluster head. For some applications, this is a reasonable assumption, especially in cases where the sensors have a significant reach. However, in cases where the sensors are very small, don't have a lot of range, and are haphazardly deployed (for instance, dropped behind an airplane, this assumption may not be valid. Also, the assumption that every node shares a key with the base station may be problematic. Distributing that many keys to a large number of nodes can present problems. Additionally, the shortened lifespan of these sensors may not make that much work worthwhile.

As an aside, this network may even be <u>more</u> prone to denial of service attacks. A node, if it is compromised, can inject bad data or a bad signature for an event, and since one MAC won't match at the base station, the base station rejects the entire event, even though there may have been t non-compromised nodes that reported the event successfully and were not compromised. However, this problem won't be detected until the packet reaches the base station, so many of the routing sensors will waste power computing and communicating this data.

For the assumptions stated and the problem presented (just preventing false data-injection, not anything else) the analysis of the security of the stages of the proposed system (Node Initialization and Deployment, Association Discovery, Report

Endorsement, En-route filtering, Base Station Verification) is very complete and thorough. The security seems to hold as long as there aren't t compromised stations, which is an important result by itself.

SA: 0, WA: 4, WR: 4, SR: 2