Chapter 3.5
Detecting Cheating Aggregators and Report Dropping Attacks in Wireless Sensor Networks

Mohit Virendra
State University of New York at Buffalo, USA

Qi Duan
State University of New York at Buffalo, USA

Shambhu Upadhyaya
State University of New York at Buffalo, USA

ABSTRACT

This chapter focuses on an important, challenging and yet largely unaddressed problem in Wireless Sensor Networks (WSN) data communication: detecting cheating aggregators and malicious/selfish discarding of data reports en route to the Base Stations (BSs). If undetected, such attacks can significantly affect the performance of applications. The goal is to make the aggregation process tamper-resistant so that the aggregator cannot report arbitrary values, and to ensure that silent discarding of data reports by intermediate en-route nodes is detected in a bounded fashion. In our model, individual node readings are aggregated into data reports by Aggregator Nodes or Cluster Heads and forwarded to the BS. BS performs a two-stage analysis on these reports: (a) Verification through attached proofs, (b) Comparison with Proxy Reports for ensuring arrival accuracy. Proofs are non-interactive verifiers sent with reports to attest correctness of reported values. Proxy Reports are periodically sent along alternate paths by non-aggregator nodes, piggybacked on data reports from other nodes. The model is intended as a guide for implementing security in real sensor network applications. It is simple and comprehensive, covering a variety of data formats and aggregation models: numeric and non-numeric data and aggregators located across one or multiple hops. Security analysis shows that the reports, both primary and proxy, cannot be forged by any outsiders and the contents of the reports are held confidential and the scheme is robust against collusion attacks. Lightweight design aims at minimal additional control and energy overhead. Simulation results show its fault tolerance against random and patterned node failures.

DOI: 10.4018/978-1-61350-101-6.ch305

INTRODUCTION

Wireless Sensor Networks (WSNs) are finding increased application in data collection operations, especially in hostile terrains, wartime operations and in emergency responder systems. Aerial scattering or similar quick and infrastructure-less installation of sensor nodes and strategic positioning of Base Stations (BSs) allows rapid network deployment. Individual sensor readings are aggregated into data reports by Aggregator Nodes (ANs) or Cluster Heads (CHs) and forwarded to the BSs. Data collected at the BS in such scenarios may be critical for decision making (e.g., tracking moving enemy targets). Any en route data tampering or data loss will result in inaccurate collection at the BS and significantly affect the underlying decision making process besides depleting the nodes' battery power (Karlof & Wagner, 2003) . Admissible robustness and dependability in data reporting are thus desirable.

Wireless channel constraints, computational capability of sensor nodes and battery power issues are inhibitors to attaining these goals. Adverse ambient deployment conditions may additionally magnify the impact of any attacks or Byzantine failures in the network, enhancing the success-probability for an adversary.

1.1 Threat Model and Problem Definition

WSN security research has chiefly concentrated on key management, secure broadcast, Sybil attacks and false data injection attacks (Zhu et al, 2004) (Chan et al, 2003)(Chan, 2005)(Newsome, 2004). Even though these schemes assume data reports to be end-to-end encrypted between aggregators and BS, the reports may still be:

- *Misaggregated* in the first place by cheating aggregators (Wu,2006)or compromised aggregators(Perrig, 2003)and this may go undetected if aggregation occurs across multiple hops, or
- Selectively dropped by malicious aggregators or other intermediate nodes along the path to the BS

Such miasggregation and discarding are very simple exploits which abuse the basic open-air property of the wireless channel. It would be very hard to distinguish genuine data-aggregation, in-network-processing and passive-participation operations[1] from malicious altering or arbitrary discarding of data reports. These hard-to-detect attacks constitute the system-centric threat model of our chapter.

For better understanding, we formally define *Misaggregation* and *Report Dropping* Attacks as follows:

- **Misaggregation:** ANs/CHs deliberately send incorrect values in the data reports to the BS. This attack is especially relevant when the aggregation occurs across more than one wireless hops (large clusters); not all the nodes in the aggregation group or cluster can "hear back" and verify the reports forwarded to the BS by the aggregator.
- **Report Dropping:** Intermediate nodes en route to the BS deliberately and unnecessarily drop data reports to skew/adversely-affect the data collection process at the BS.

The BS should be able to detect in a determinate fashion if node readings are deviant (indicating anomalies in the aggregation process, possibly due to aggregators reporting incorrect values). It should be able to pinpoint cheating/misreporting aggregators and be able to detect any malicious extraneous/superfluous/unnecessary dropping or discarding of reports as well. Both these problems are considered collectively because their solution achieves the same end goal: reducing incorrect data collection at the BS (It is seen eventually