Chapter XXXVIII
Resilience Against False Data Injection Attack in Wireless Sensor Networks

Miao Ma
The Hong Kong University of Science and Technology, Hong Kong

ABSTRACT

One of the severe security threats in wireless sensor network is false data injection attack, that is, the compromised sensors forge the events that do not occur. To defend against false data injection attack, six en-route filtering schemes in a homogeneous sensor network are described. Furthermore, one sink filtering scheme in a heterogeneous sensor network is also presented. We find that deploying heterogeneous nodes in a sensor network is an attractive approach because of its potential to increase network lifetime, reliability, and resiliency.

INTRODUCTION

Wireless sensor networks (WSN) usually consist of a large number of inexpensive and small nodes with sensing, data processing, and communication capabilities. These nodes are densely deployed in a region of interest and collaborate to accomplish a common task, such as environmental monitoring, military surveillance, and industry process control. Distinguished from traditional wireless networks and ad hoc networks, WSN are featured in dense node deployment, unreliable sensor node, frequent topology change, limited power resource, and limited computation capacity, restricted memory space. These unique characteristics and constraints present many new challenges to the design and implementation of WSN.

For many mission-critical applications, the sensor nodes are deployed in an unattended or often hostile environment and WSN face many security and privacy challenges. One challenge is that when deployed in hostile environments, sensor nodes may be captured or compromised by the adversaries. Then the adversaries can obtain the secret keys

stored in the compromised nodes, and misuse them to launch *insider attacks*. Therefore, a nonresilient security protection scheme will exhibit a *threshold breakdown* problem. That is, the design is secure against t or less compromised nodes, but once more than t nodes are compromised the security design completely breaks down, where t is a fixed threshold. Since in reality nobody can prevent an attacker from compromising more than t nodes, such a security protection solution cannot meet the resilience requirement. Our expectation in terms of resilience is that, compromising t nodes in a certain area can only enable an adversary to forge nonexisting events in that specific area, rather than any other location at all. Put in other words, for an attacker, the only way to generate a valid report on a nonexisting event happening in a certain area is to compromise t nodes in that area.

In this chapter, we overview several schemes that have been proposed to defend against *compromised nodes*. We will show that several schemes are only resilient against a small, fixed number of compromised nodes with threshold breakdown problems, while subsequent schemes partially and completely solve the threshold breakdown problems.

The rest of this chapter is organized as follows. In the next section, we introduce the background. Several en-route filtering schemes in a homogeneous sensor network are presented. Furthermore, a sink filtering scheme in a heterogeneous sensor network is shown. Finally, the last section concludes the chapter.

BACKGROUND

False Data Injection Attacks

We consider a sensor network, which consist of hundreds or thousands of low-cost sensors. Each sensor senses and collects data from the environment. There is at least one base station (or *sink*), which is typically a resource-abundant computer equipped with sufficient computation and storage capabilities. We assume that the sensor nodes are deployed in a high density, so that once an event happens it can be detected by multiple sensors. However, it is inefficient and also unnecessary for every sensor node to report their raw data to the sink node, because: (1) every data packet usually needs to travel many hops (e.g., tens or event longer) to reach the sink; (2) each sensor node is often constrained by scarce resources in memory, computation, communication, and battery; and (3) in many cases there is high redundancy in the raw data. Hence, raw data are often fused and aggregated locally, and only the aggregated information is returned to the sink. In such a setting, certain nodes in the sensor network will function as *cluster heads* (*CHs*), to collect the raw sensing data from the sensors, process it locally, and return the aggregation report to the sink. Once the sink receives an event report, it may take action accordingly.

Unfortunately, the above event detection and reporting process can be seriously threatened by *false data injection attacks*. As we stated above, sensors are usually deployed in unattended or even hostile environments, and an adversary may capture or compromise sensor nodes. Once this happens, the compromised nodes can easily inject false data reports of nonexisting events. Even worse, when an adversary compromises more nodes and combines all the obtained secret keys, the adversary can freely forge the event reports which not only "happen" at the locations where the nodes are compromised, but also at *arbitrary* locations in the field. These fabricated reports not only produce false alarms (and lead to *false positives*), but also waste valuable network resources, such as energy and bandwidth, when delivering the forged reports to the base station. Therefore, it is important to design an effective filtering scheme to defend against such attacks and minimize their impacts.

In this chapter, we consider the following *threat* model. The attacker may compromise multiple sensor nodes in the network, but cannot compromise the sink. Once a sensor node is compromised, the attacker can obtain all secret keys, data, and codes stored in the sensor. Whenever more nodes are compromised, the attacker can combine all the secret keys that have obtained, and can also load a compromised node with the secret keys obtained