Chapter 15

On Situational Aware En–Route Filtering against Injected False Data in Cyber Physical Systems

Xinyu Yang
Xi’an Jiaotong University, P. R. China

Jie Lin
Xi’an Jiaotong University, P. R. China

Wei Yu
Towson University, USA

Xinwen Fu
University of Massachusetts Lowell, USA

Genshe Chen
Independent Consultant Professional, USA

Erik P. Blasch
Air Force Research Laboratory, USA

ABSTRACT

Cyber-physical systems (CPS) are systems with a tight coupling of the cyber aspects of computing and communications with the physical aspects of dynamics and engineering that abide by the laws of physics. The real-time monitoring provided by wireless sensor networks (WSNs) is essential for CPS, as it provides rich and pertinent information on the condition of physical systems. In WSNs, the attackers could inject false measurements to the controller through compromised sensor nodes, which not only threaten the security of the system, but also consume significant network resources and pose serious threats to the lifetime of sensor networks. To mitigate false data injection (FDI) measurement attacks, a number of situation aware en-route filtering schemes to filter false data inside the networks have been developed. In this book chapter, the authors first review those existing situation aware en-route filter mechanisms such as: Statistical En-route Filtering (SEF), Location-Based Resilient Secrecy (LBRS), Location-ware End-to-end Data Security (LEDS), and Dynamic En-route Filtering Scheme (DEFS). The authors then compare the performance of those schemes via both the theoretical analysis and simulation study. These extensive simulations validate findings that most of the schemes can filter out false data within few hops, and the filtering efficiency increases as the number of hops increases and the filtering efficiency of most schemes decreases rapidly as the number of compromised nodes increases.

DOI: 10.4018/978-1-4666-0104-8.ch015
INTRODUCTION

Monitoring and controlling physical systems through geographically distributed sensors and actuators have become an important task in numerous environment and infrastructure applications. These applications have received a renewed attention because of the advances in sensor network technologies and new development in cyber-physical systems (CPS) (CPSweek, 2010). To monitor and control the physical systems, a typical CPS integrates sensor nodes, actuators, controllers, and networks. In a CPS system, sensor nodes obtain the measurement from the physical components, process the measurements, and send measured data to the controller through computer networks. According to these measurements, the controller estimates the states of physical systems and sends feedback commands to the actuators, which control the operation of physical systems. Thus, the real-time monitoring provided by wireless sensor networks (WSN) is essential for CPS, as it provides rich and pertinent information on the condition of physical systems.

WSNs are important components in CPS and are formed by a set of resource-constrained sensor nodes communicated through an ad hoc fashion. In WSNs, sensor nodes usually are deployed in unattended or even harsh environments (e.g., battlefield) and the lack of tamper-resistance hardware increases the possibility of nodes to be compromised by attackers. Once nodes are compromised, the secret information stored in nodes becomes visible to the attackers. Even worse, the attackers could launch false data injection attacks via compromised nodes, consuming significant network resources and posing serious threats to the lifetime of sensor networks (Ye, 2004; Chen, 2009). In particular, the false data injected by compromised nodes can lead to false events and affect the decisions made at the sink of WSNs. Because a large amount of false data injected by compromised nodes are transmitted to the sink via multiple-hop routes, the false data increases the communication overhead of energy-limited nodes and ultimately shortens the lifetime of WSNs.

To mitigate the false data injection (FDI) type of attacks, we shall develop the situation aware filtering schemes to filter out false injected data inside the network before arriving at the sink of WSNs (or the key controller of CPS). Note that situational awareness (SA) is commonly described as knowing what is going on around the system and within that knowledge of surroundings and being able to identify which events in those surroundings are important (Shen 2007, Shen 2009). Hence, we shall continue to monitor system performance and threats and develop techniques for accurate analysis, fast detection and response against threats. Following this design principle, a number of the situations aware en-route filtering schemes to filter false data injected from the compromised nodes have been developed.

The basic idea of situation aware en-route filtering is based on T-authentication. That is, a legitimate data report must carry at least T valid message authentication codes (MACs) generated by different nodes within the network. T is a threshold and predefined before WSN is deployed. Generally speaking, MAC is a small fixed-size block of data generated based on the message M and a shared authentication key K, and used to be attached in message M and allow the receiver to authenticate the integrity of message M. The formula of MAC generation is denoted as $MAC = F(M, K)$, where $F(.)$ is the MAC generation function. Various MAC generation approaches have been studied in the past, including Cipher Block Chaining (CBC-MAC), One-key (OMAC), and Hash-based (HMAC) and others. The detailed description of MAC generations approach is beyond the scope of this book chapter, and readers can find more details in (Block, 2002; T. Iwara, 2002; H. Krawczyk, 1997). In terms of the false date en-route filtering schemes studied in this chapter, when a report is transmitted to the sink along the route, each forwarding node determines whether $T$ valid MACs are attached to the report.