Chapter 3
A Forward & Backward Secure Key Management in Wireless Sensor Networks for PCS/SCADA

Hani Alzaid
Queensland University of Technology, Australia & King Abdulaziz City for Science and Technology, Saudi Arabia

Dong Gook Park
Sunchon National University, South Korea

Juan Gonzàlez Nieto
Queensland University of Technology, Australia

Colin Boyd
Queensland University of Technology, Australia

Ernest Foo
Queensland University of Technology, Australia

ABSTRACT

Process Control Systems (PCSs) or Supervisory Control and Data Acquisition (SCADA) systems have recently been added to the already wide collection of wireless sensor network applications. The PCS/SCADA environment is somewhat more amenable to the use of heavy cryptographic mechanisms such as public key cryptography than other sensor application environments. The sensor nodes in this environment, however, are still open to devastating attacks such as node capture, which makes the design of secure key management challenging. This chapter introduces an adversary model with which we can assess key management protocols. It also proposes a key management scheme to defeat node capture attack by offering both forward and backward secrecies. The scheme overcomes the pitfalls of a comparative scheme while being not computationally more expensive.

DOI: 10.4018/978-1-60960-027-3.ch003

INTRODUCTION

Process Control Systems (PCSs) or Supervisory Control and Data Acquisition (SCADA) systems are used to monitor and control a plant or equipment in industries such as energy, oil and gas refining, and transportation. SCADA systems enable the transfer of data between the network manager and a number of Remote Terminal Units (RTUs), sensor nodes, etc. A SCADA system gathers critical information (such as where a leak in a pipeline has occurred) and then transfers this information back to the network manager. The network manager is responsible for alerting the home station about the leak and carrying out necessary analysis such as determining whether the leak is critical or not.

Owners and operators of SCADA systems aim to increase the monitoring sensitivity of their systems and reduce the day to day running cost wherever possible. The intelligent monitoring capabilities of Wireless Sensor Networks (WSNs) mean that integration between SCADA and WSNs can be one way to achieve these aims. WSNs facilitate the monitoring process by performing specific tasks such as sensing physical phenomena at a remote field and then reporting them back to the network manager. They can form the "eyes and ears" of SCADA systems. Nodes, which are capable of performing functions such as gas detection and temperature sensing, provide information that can tell an experienced operator how well oil/gas pipelines are performing.

Roman et al. highlighted the role that WSNs can play in SCADA (2007). They argued that WSNs can aid the functionality of SCADA systems by providing monitoring, alerts, and information on demand. However, security vulnerabilities can be introduced to SCADA systems by WSNs. One of these potential vulnerabilities is the security compromise of sensor nodes, given the lack of tamper resistant packaging (Hartung, Balasalle & Han, 2005). By gaining physical access, an adversary can gain control of one or more sensor nodes and readily access sensitive information such as keys or passwords. The adversary can therefore easily get access to the plain text of encrypted messages that are routed through the compromised nodes -- compromising data confidentiality. The adversary may also inject its own commodity nodes into the network by fooling legitimate nodes into believing that the commodity node is a legitimate member of the network. Another adversary activity is to launch a selective forwarding attack. In this type of attack, the node under control of the adversary selectively drops legitimate packets in order to affect the overall performance of the system (Karlof & Wagner, 2003).

In this chapter, we focus on strengthening the security level at the weakest component of the SCADA system which exists in remote fields (Beaver, Gallup, Neumann & Torgerson, 2002). The remote field has the weakest physical security requirements and consists of substations and intelligent electronic devices such as sensors, which will be discussed in Section Scada. We introduce a new model of adversary with which we can evaluate key management protocols. We then propose a new key management protocol that updates the shared symmetric key between the network manager and a sensor node or between the network manager and a group of sensor nodes. Finally, we analyze the performance of our proposal and compare it with those of Nilsson et al.'s scheme (Nilsson, Roosta, Lindqvist & Valdes, 2008). This performance analysis covers memory overhead, communication cost, and computation cost for these schemes.

SCADA

To best understand the added value of the proposed scheme, some understanding of SCADA is in order. Today's SCADA systems (the third generation) are a combination of legacy and modern technology (McClanahan, 2003). The third generation SCADA has become an open system