Chapter 44
Secure Key Establishment in Wireless Sensor Networks

Suman Bala
Thapar University, India

Gaurav Sharma
Thapar University, India

Anil K. Verma
Thapar University, India

ABSTRACT

Over the last two decades, advancement in pervasive sensing, embedded computing and wireless communication has lead an attention to a new research area of engineered systems termed as Cyber-Physical Systems (CPS). CPS has bridged the gap between the physical world to the cyber world. It is envisioned that Wireless Sensor Networks (WSN) plays an important role in the actuality of CPS. Due to wireless communication in WSN, it is more vulnerable to security threats. Key establishment is an approach, which is responsible for establishing a session between two communicating parties and therefore, a lightweight key establishment scheme is essential. In this chapter, we review the state of the art of these solutions by discussing key establishment in WSN. Also, a discussion has been carried out to capture few challenges in implementing them in real and future research directions in this area are explored to transport the field to an improved level.

INTRODUCTION

Computation and communication are two key potentials that will control the physical world. A cyber-physical system (CPS) is an amalgamation of operations like monitor, coordinate, control, computation, communication of the physical entities to bridge the cyber world. The coordination of cyber system and physical entities will lead to the reality of dust particle world to the network of large-scale systems. CPS would foster sensor network as a typical CPS consists of numerous sensors and actuator networks. So, it would be necessary to review the developments in sensor networks to project the developments in CPS.

DOI: 10.4018/978-1-5225-5634-3.ch044

Today's industrial and economic growth is totally dependent on cyber-physical systems. With the help of Internet a lot has been changed. In last two decades, the way of information gathering, processing, storing and retrieval is totally changed. It has also changed the approach of interaction and communication with machines. A typical CPS consists of multiple wireless sensor networks, for example a greenhouse management system, which can control the system with heating, watering, lighting, cooling, fertilizing, generation of carbon dioxide as subsystems. For this, the intensity of light, density of carbon dioxide, temperature and humidity need to be captured, computed and transmitted.

WSN consists of large number of motes, which can capture the physical entity from the environment, processing it to digital format and transmitting to the base station. WSN facilitates various applications such as habitat monitoring, health care, environment monitoring, military operations etc. In WSN, the data is transmitted over an open network; various security measures need to be employed to prevent eavesdropping of credentials by adversaries. This can be accomplished by the use of cryptographic mechanisms to assure fundamental security properties like confidentiality, integrity and authenticity. All cryptographic primitives require secret keys for the encryption/decryption of the message. The distribution of secret key or the establishment of secret key should be secure. Key management is such technique, which can support key establishment and key maintenance among authorized parties.

In spite of prospective features of WSN, they have major resource constraints in terms of limited storage, power, processing and transmission (computation and communication) capabilities. This reflects on the construction of the algorithms, there is always a trade off between security and storage, or computation and communication.

In this chapter, we review the state of the art of key establishment for WSNs based on two approaches, symmetric and asymmetric. We evaluate these approaches based on metrics that are of central importance in resource-constrained applications. Our objective is to identify general ideas that are responsible for the improvement of future prospects, resulting in better potential for acceptance by industry standards.

BACKGROUND

Recent engineering advances especially in the field of communications lead to an emerging world of inexpensive and mobile devices, which not only solves the purpose of checking email and browsing on the go but also provides various kinds of useful applications like vehicles tracking, industrial production processing, environment conditions monitoring, patient health monitoring, battlefield surveillance etc.

Wireless Sensor Networks (WSN) (Akyildiz et al., 2002; Chen & Zhao, 2005; Olariu & Xu 2005) gained attention during last decade and enabled the development of low-powered sensor networks. Generally, WSN consists of a base station and large number of motes. A typical mote is equipped with integrated 8-bit microcontroller, radio transceiver, sensors such as photodiodes, thermistors, etc., 4KB of RAM, 128 KB of program space and a battery. The task of sensor mote is to gather, process and forward the physical information from the environment to the base station. WSN possess lots of security challenges. These are usually deployed in hostile areas. As sensor motes transmit information over the air, it attracts vulnerabilities, which can harm from malfunctioning of transmitted messages to physical capturing of motes.

Energy consumption is another important challenge in WSN, which has to be focused. Due to less bandwidth available for communication and low battery life span of a sensor mote, wireless transmission is expensive in terms of energy usage. There are various guidelines for providing security in WSN