Review of IoT-enabled Wireless Sensor Networks' secure key management methods

Enugala Raju[1,a] and Dr. Kadapa Sagar[2]

[1] Sumathi Reddy Institute of Technology for Women, Warangal, Telangana, India.
[2]Professor, Dept. of CSE, CBIT, Hyderabad, Telangana, India

[a] Corresponding author:raju.cse999@gmail.com

Abstract: with the hasty growth and extensive use of wireless sensor networks (WSNs), it is imperative to enhance the security for WSNs. The concept of the Internet of Things (IoT) is determined by growths of the Internet with the interconnectedness of diversified smart objects using dissimilar networking and communication technologies. Among countless basic networking technologies for the IoT, Wireless Sensor Network (WSN) technology has become an essential building block. IoT empowered sensor networks to afford a wide variety of application areas such as smart homes, smart healthcare, smart cities and various solutions for the manufacturing industry. The incorporation of WSNs in IoT will also generate newfangled security challenges for launching secure channels sandwiched between low power sensor nodes and Internet hosts. The key management is an effective way to protect WSNs from various malicious attacks. This will lead to numerous challenges in designing new key establishment and authentication protocols. This paper discusses about several KMS Taxonomies and surveys and recent KMS which are applicable for WSN.

Keywords: Wireless Sensor Networks, Internet of Things, Authentication, Key Management schemes

INTRODUCTION

A technological advance called the Internet of Things integrates different wired and wireless network types to the Internet, interconnecting various objects with one another and establishing a massive network for monitoring, analysing, and controlling. WSN is composed of tiny sensors and is used even in distant regions such as aquatic, agricultural, and forest areas. The affordability, memory, and networking capabilities of these sensors are all minimal. It is an important factor of the IoT sensor layer, that serves as a deep extension of the existing network and an extremely important basis for the growth of IoT, and is used in a wide range of applications which includingmilitary applications, acoustic, traffic surveillance, industrial and agriculture manufacturing. To simplify secure communication, WSN sensors should transmit data confidentially from one sensor to another or to the Base Station (BS). The lack of protection may expose the sensor network to vulnerable attacks. Data confidentiality is ensured through data encrypting and decipherment. Numerous keys have been involved in this process in general, and these keys must be distributed and managed carefully among sensors.

Features of Wireless Sensor Network

Limited Resources. Sensor nodes have incredibly limited resources needed.
Large-Scale Networks. Large scale is reflected in two aspects: The sensor nodes are placed with greater density, and the sensor network covers a larger space. The sensor network can acquire more precise and comprehensive data in this way. The information quality and accuracy requirements for each node sensing data can both be reduced and increased by aggregating data from a large number of nodes [1]. The availability of redundant nodes in a large-scale multinode distributed deployment can enhance the fault resilience of wireless sensor networks.