Chapter 3
A Review of Cryptographic Algorithms for the Internet of Things

Issmat Shah Masoodi
University of Kashmir, India

Bisma Javid
University of Kashmir, India

ABSTRACT

There are various emerging areas in which profoundly constrained interconnected devices connect to accomplish specific tasks. Nowadays, internet of things (IoT) enables many low-resource and constrained devices to communicate, do computations, and make smarter decisions within a short period. However, there are many challenges and issues in such devices like power consumption, limited battery, memory space, performance, cost, and security. This chapter presents the security issues in such a constrained environment, where the traditional cryptographic algorithms cannot be used and, thus, discusses various lightweight cryptographic algorithms in detail and present a comparison between these algorithms. Further, the chapter also discusses the power awakening scheme and reference architecture in IoT for constrained device environment with a focus on research challenges, issues, and their solutions.

DOI: 10.4018/978-1-5225-5742-5.ch003

INTRODUCTION

In recent years, the Internet of Things has witnessed rapid growth and is being perceived as hypernym for interconnected technologies, objects, devices, and services. Nevertheless, after years of contribution to this research, there is still no clear and universal definition of the concept. However, still, the application frameworks and opportunities offered in the market by objects are communicating actively far beyond specific horizons. The novel contributions, new applications, and services conceived by innovators and researchers are bewildering and clearly show the high and vast opportunities for our next generations. In the early 2000s, RFID technology was designed and developed mainly across the engineering sector for tracking and tracing goods. At the same time, research was conducted on sensor networks and miniaturized smart systems. The size of sensors was becoming very small and computing power dramatically increased. Nevertheless, innovative solutions were always developed and provided for specific application cases, and there was no absolute interconnectivity and interoperability between different application areas. For example, fields like logistics and manufacturing are well-known as they provide an immediate business benefit regarding asset tracking and supply chain management. However, real solutions cannot be applied to other fields such as demotics, where business synergies can provide services with obvious added-value benefits. As the IoT zone covers such a vast spectrum of application fields, the happening cycles and technologies used can be completely classified. Often, the developments in technology are driven by idealistic, tiny and medium-sized enterprises (SME) that try to meet targets try to catch ongoing trends at a faster pace. However, the target is usually an output within a narrow scope, the solutions are usually non-interoperable, and while successful, they are unable to produce a common abstract infrastructure capable of marking notable progress in the whole field. This holds for large-scale companies that usually develop dedicated solutions for specific business opportunities without implementing applicable concepts. Therefore, current solutions can still be seen as peaceful solutions, that can implement some "INTRAnet of Things" despite "INTERnet of Things." While being logical regarding the point, in the long term, the prevailing situation is unsustainable. Nowadays, we can observe a situation of a similar sort to that in the networking field, where at its infancy many solutions are obtained but were subsequently discarded in favor of a unified communication infrastructure, the TCP/IP protocol suite. We do believe that different classes of devices will always co-exist. Taxonomies are to be created according to various principles, such as critical or non-critical, or distributed or centralized. These classes can promote different profiles as per the specific needs and requirements of domains and applications. By the reference model, we mean an abstract framework that comprises at least a set of unifying concepts and relationships for understanding